

**GOVERNMENT OF ZAMBIA**

STATUTORY INSTRUMENT NO. 9 OF 2016

**The Financial Intelligence Centre Act, 2010  
(Act No. 46 of 2010)**

**The Financial Intelligence Centre (General)  
Regulations, 2016**

ARRANGEMENT OF REGULATIONS

*Regulation*

**PART I**

**PRELIMINARY PROVISIONS**

1. Title
2. Interpretation

**PART II**

**COLLECTION AND DISSEMINATION OF INFORMATION**

3. Dissemination and disclosure of suspicious transactions
4. Access to information
5. Request for Information
6. Freezing account and suspending transaction

**PART III**

**CUSTOMER DUE DILIGENCE MEASURES**

7. Identification and verification of customer identity
8. Risksensitive application of customer due diligence and other measures
9. Low risk of money laundering or terrorist financing
10. High risk of money laundering or terrorist financing
11. Reliance on identification by third party

**PART IV****RISK MANGEMENT**

12. Risk management systems
13. Internal programmes to combat money laundering, financing of terrorism and other serious crimes
14. Measures for business relations and transactions from countries that do not apply international standards

**PART V****GENRAL PROVISIONS**

15. Reporting suspicious transactions
16. Oath and affirmation
17. General Offence and penalty

**SCHEDULES**

IN EXERCISE of the powers contained in section *fifty eight* of the Financial Intelligence Centre Act, 2010, and in consultation with the Centre, the following Regulations are made:

## PART I

### PRELIMINARY PROVISIONS

- |  |                |
|--|----------------|
| 1. These Regulations may be cited as the Financial Intelligence Centre (General) Regulations, 2015.  | Title          |
| 2. In these Regulations, unless the context otherwise requires   | Interpretation |
| <p>“account” has the meaning assigned to it in the Act;</p> <p>“beneficial owner” has the meaning assigned to it in the Act;</p> <p>“Centre” means the Financial Intelligence Centre established under section <i>three</i> of the Act;</p> <p>“close associate” includes an individual who</p> <p style="padding-left: 20px;">(a) is known to have joint beneficial ownership or control of a legal entity or legal arrangement, or any other close business relation, with a politically-exposed person; and</p> <p style="padding-left: 20px;">(b) has sole beneficial ownership or control of a legal entity or legal arrangement which is known to have been set up for the benefit of a politically-exposed person;</p> <p>“control” means a situation where</p> <p style="padding-left: 20px;">(a) one person or two or more persons acting in concert, directly or indirectly owns, controls or has the power to vote twenty-five percent or more of any class of voting shares of another person;</p> <p style="padding-left: 20px;">(b) one person, or a combination of two or more persons acting in concert, controls in any manner, the election of a majority of the directors, trustees or other persons exercising similar functions of another person; or</p> <p style="padding-left: 20px;">(c) circumstances exist that indicate that one person, or a combination of two or more persons acting in concert, directly or indirectly, exercises a controlling influence over the management, policies or affairs of another person;</p> <p>“Council” means a city, municipal or district council established under the Local Government Act;</p> |                |

Cap 281

“customer” has the meaning assigned to it in the Act;

“Director” means the Director of the Centre appointed under section *nine* of the Act;

“Egmont Group” means the international network of financial intelligence units (FIUs) established to promote and enhance international cooperation information sharing among financial intelligence units relating to the fight against money laundering and the financing of terrorism;

“high-risk customer” includes

- (a) a non-resident customer;
- (b) a private banking customer;
- (c) a legal person or legal arrangement that is a personal-asset holding vehicle;
- (d) a politically-exposed person;
- (e) a company that has a nominee shareholder or shares in bearer form; or
- (f) a customer that performs a transaction on behalf of another person, whether the identity of such other person is disclosed or not.

“immediate family member” in relation to an individual includes

- (a) a spouse;
- (b) a sibling;
- (c) a child and were applicable the spouse of a child; and
- (d) a parent;

“law enforcement agency” has the meaning assigned to it in the Act;

“politically-exposed person” means

- (a) an individual who holds, or has held, public office, and includes
  - (i) a Head of State or Government;
  - (ii) a Minister;
  - (iii) a Deputy Minister;
  - (iv) a politician;
  - (v) a political party official;
  - (vi) a judicial official or other senior official of a quasi-judicial body;
  - (vii) a military official;
  - (viii) a member of an administrative, management or supervisory body of a State owned enterprise;

- (b) an individual who is, or has been, entrusted with a public function by a State, public body or a local or international organisation;
- (c) an immediate family member of a person referred to in paragraph (a); or
- (d) a close associate of a person referred to in paragraph (a);

“public body” has the meaning assigned to it in the Act;

“public function” means a function performed by a public officer in a public body in an official capacity in relation to the public body;

“public officer” means a person employed or performing a function in a public body;

“reporting entity” has the meaning assigned to it in the Act;

“statutory corporation” means a body corporate wholly or partly owned by the Government;

“supervisory authority” has the meaning assigned to it in the Act;

“suspicious transaction report” has the meaning assigned to it in the Act; and

“transaction” has the meaning assigned to it in the Act.

## PART II

### ACCESS AND DISSEMINATION OF INFORMATION

- |   |  |
|---|--|
| <p>3. The Centre shall disseminate and provide information relating to suspicious transactions to a law enforcement agency or foreign designated authority for purposes of the Act in Form I set out in the First Schedule.</p>   | <p>Dissemination and disclosure of suspicious transactions</p> |
| <p>4. The Centre may, in exercising its functions under the Act, use electronic communications services to access, directly or indirectly, on a timely basis, financial, administrative and law enforcement information.</p>  | <p>Access to information</p>                                   |
| <p>5. The Director shall request a reporting entity to provide financial information, in Form II set out in the First Schedule.</p>   | <p>Request for information</p>                                 |
| <p>6. (1) The Director shall order a reporting entity to freeze an account or suspend a transaction in Form III set out in the First Schedule.</p> <p>(2) The Centre shall serve a signed copy of a freezing or suspension order in Form III on a reporting entity where the account is held or the transaction is processed or intended to be processed.</p> | <p>Freezing account and suspending transaction</p>             |

- (3) A reporting entity shall, upon receipt of the freezing or suspension order issued under sub-regulation (1)ô
- (a) stop all activity on the account concerned; and
  - (b) suspend the specified transaction for the duration specified in the order.
- (4) An order issued under this regulation shall remain in force until ô
- (a) the expiration of a period of ten days from the date of its issuance;
  - (b) the Director issues an order discharging the freezing or suspension order in Form IV set out in the First Schedule; or
  - (c) a judge issues an order discharging the freezing or suspension order issued by the Director.
- (5) The Centre may, for purposes of monitoring compliance, request a reporting entity to submit a statement of an account from the date of issuance of a freezing or suspension order to the date of discharge of the order.

### PART III

#### CUSTOMER DUE DILIGENCE

Identification and verification of customer identity

7. (1) A reporting entity shall verify its customer's identity as follows:
- (a) for an individual, the reporting entity shall verify the full name, date and place of birth, address and other particulars of the individual by comparing the particulars withô
    - (i) the individual's driving licence, passport or national identification document bearing the individual's pictorial image;
    - (ii) a reference from the individual's employer or a professional or customary authority that has known that individual for at least a year;
    - (iii) references obtained from the individual's foreign bank, where possible, in the case of a nonresident or foreigner;
    - (iv) information obtained through a credit reference agency search;
    - (v) an original or certified true copy of the latest Council or applicable rates, or utility bill receipt; and

- (vi) information which is obtained from any other independent source, if it is accurate and reasonably necessary taking into account any other law or guidelines concerning the verification of identities;
- (b) for a body corporate—
- (i) by comparing the submitted details of the body corporate with a certified true copy of its certificate of incorporation issued by the Registrar of Companies or another relevant authority;
  - (ii) reviewing the tax payer identification number (TPIN) issued by the Zambia Revenue Authority and other information held by the Register of companies or other relevant register; and
  - (iii) except for statutory bodies, the particulars of every person exercising direct or indirect control, for the purposes of identifying the beneficial owner; and
- (c) for a partnership, obtain from an individual acting or purporting to act on its behalf—
- (i) the name of the partnership;
  - (ii) the business address;
  - (iii) the partnership agreement; and
  - (iv) the full names, address and date and place of birth of every partner, including the person who exercises direct or indirect control or management of the partnership, for purposes of identifying the beneficial owner.

(2) The requirements prescribed in sub-regulation (1) apply to an individual acting on behalf of the customer in establishing an account or a business relationship with a reporting entity.

(3) Where the legal arrangement is a trust, a reporting entity shall verify the particulars obtained in respect of the trust by comparing the name of the trustees, the settler and beneficiary of express trust with the trust deed or other founding document in terms of which the trust is created.

(4) Where an individual, legal person or legal arrangement is deceased or ceases to exist respectively, a reporting entity shall verify the particulars referred to in this regulation by comparing those particulars with information that can reasonably be utilised to achieve such verification and is obtainable by reasonably practicable means, taking into account any other applicable law or guidelines concerning the verification of identities applicable to the reporting entity.

(5) Where an individual seeks to establish an account or a business relationship with a reporting entity on behalf of an individual, a legal person or legal arrangement, the reporting entity shall, in addition to any other step applicable in terms of subregulation (1), obtain from the individual, a power of attorney, service level agreement or other proof of that individual's authority to act on behalf of the individual, legal person or legal arrangement.

(6) A reporting entity shall update customer bank mandates periodically in order to ensure that the verification process provides accurate information for purposes of the Act.

(7) The updates referred to in sub-regulation (6) shall be occasioned by a change in

- (a) the authorised signatories;
- (b) the purpose of the account;
- (c) the scope of terms and conditions applicable to account; and
- (d) any other material aspect of, or likely to affect, an account.

Risk-sensitive application of customer due diligence and other measures

8. A reporting entity may adapt the nature and extent of application of the customer due diligence measures specified in regulation 7 commensurate with the level of the money laundering and terrorist financing risk associated with the customer, business relationship or transaction.

Low of risk money laundering or terrorist financing

9. (1) A reporting entity may apply the simplified customer due diligence measures specified in the Second Schedule where the reporting entity determines that the risk of money laundering or terrorist financing is low.

(2) Where a reporting entity applies simplified customer due diligence measures, the reporting entity shall prove the low risk to the satisfaction of the Centre or the supervisory authority.



(3) A reporting entity shall, where the risk factors are identified in relation to a customer as set out in the Second Schedule, complete the verification of the customer's identity as soon as reasonably practicable after the commencement of the business.

10. A reporting entity shall apply the enhanced identification, verification and ongoing due diligence measures set out in the Second Schedule when dealing with high risk customers or in circumstances where the reporting entity reasonably considers the risk of money laundering or terrorist financing to be high.

High of risk  
money  
laundering or  
terrorist  
financing

11. (1) A reporting entity may rely on a third party established in, or subject to the jurisdiction of the following states to perform customer identification:

Reliance on  
identification  
by third  
party

(a) states that have established financial intelligence units which are members of the Egmont Group;

(b) states that are not subject to monitoring by the Financial Action Task Force's (FATF's) International Co-operation Review Group or Regional Review Group; and

(c) states that are not subject to United Nations sanctions.

(2) Where a reporting entity relies on a third party to perform customer identification, the reporting entity shall, immediately provide the Centre with

(a) the contract or agreement between the reporting entity and third party;

(b) the third party's

(i) full name, if the third party is an individual; or

(ii) registered name, if the third party is a body corporate or unincorporated body of persons;

(c) the name under which the third party conducts business;

(d) the full name and contact particulars of the individual who exercises control over access to copies of the customer identification information and other documents relating to the conduct of due diligence;

(e) the address where the information and documents are kept; and

(f) the full name and contact particulars of the individual who liaises with the third party on behalf of the reporting entity concerning the retention of any information and documents.

(3) Where a reporting entity relies on a third party to perform customer identification, the reporting entity shall ensure that the third party maintains copies of customer identification information and other documents relating to the conduct of due diligence for at least ten years from the end of the business relationship between the reporting entity and its customer.

#### PART IV

##### RISK MANAGEMENT

Risk  
management  
systems

12. (1) A reporting entity shall implement risk management systems to identify high risk customers whose activities may pose a high risk of money laundering and financing of terrorism including

(a) enhanced identification of high risk customers or activities engaged in by high risk customers, by taking into account

- (i) the nature and business of the customer;
- (ii) customer activities, transaction patterns and operations;
- (iii) the geographic location of the customer or transaction;
- (iv) the magnitude of customer assets that a reporting entity handles;
- (v) third parties that are or may be involved in the customer's activities;
- (vi) the beneficial ownership of an entity and the impact on risk;
- (vii) the volume of cash used by a customer in transactions;
- (viii) any other indicator that may be relevant; and

(b) enhanced verification and enhanced ongoing due diligence of high risk customers including

- (i) seeking additional information to substantiate the customer's identity or the beneficial ownership of an entity; and
- (ii) obtaining additional information about the intended nature, purpose and value of a given transaction.

13. The type and extent of measures that a reporting entity undertakes for the prevention of money laundering, financing of terrorism and any other serious offence is risk-based and includes

- (a) identifying the money laundering and terrorist financing risks that are relevant to the business in which the reporting entity is engaged;
- (b) assessing the identified risks;
- (c) designing and implementing controls to manage and mitigate the assessed risks;
- (d) monitoring and improving the effective operation of the controls;
- (e) keeping a record of the process indicated in paragraphs (a) to (d); and
- (f) establishment and implementation of a policy based on the assessed risks which sets out procedures that a reporting entity implements for carrying out appropriate identification, verification, customer due diligence and ongoing monitoring.

Internal programmes to combat money laundering, financing of terrorism and other serious crimes

14. (1) A reporting entity shall with regard to business relations and transactions with persons and arrangements from or in countries that do not, or insufficiently, apply the relevant international standards to combat money laundering, the financing of terrorism and any other serious offence

- (a) take into account risks arising from the deficiencies in the regime for combating money laundering, the financing of terrorism and any other serious offence in any given country;
- (b) consider publicly available information for identifying countries that do not, or insufficiently, apply the relevant international standards to combat money laundering, the financing of terrorism and any other serious offence; and
- (c) examine the background and purpose of transactions.

Measures for business relations and transactions from countries that do not apply international standards

(2) A reporting entity shall, if a transaction has no apparent economic or lawful purpose, examine the background and purpose of the transaction, record the findings and retain the record and submit, upon request, to the Centre, a supervisory authority or law enforcement agency.

PART V  
GENERAL PROVISIONS

Reporting  
suspicious  
transactions

15. (1) A report of a suspicious transaction shall be made in Form V set out in the First Schedule and submitted to the Centre by confidential cover

- (a) through electronic communication systems and services;
- (b) through a designated physical, postal or electronic mail address provided by the Centre; or
- (c) by courier or in person to the designated officer of centre.

(2) A report on a suspicious transaction shall be sent to the Centre as soon as possible but not later than three working days after a reporting entity, a director, principal officer, partner, professional or employee of a reporting entity forms a reasonable suspicion on the transaction or property.

(3) A report referred to in sub-regulation (1) shall contain a full description of the suspicious transaction and state the reason why it is considered suspicious.

Oath and  
affirmation

16. The Director shall administer oaths or affirmations in Form V set out in the First Schedule.

General  
offence and  
penalty

17. (1) A person who contravenes any provision of these Regulations for which a penalty is not provided commits an offence and is liable, upon conviction, to a fine not exceeding two thousand five hundred penalty units or to imprisonment for a period not exceeding one year, or to both.

(2) Where an offence under these Regulations is committed by a body corporate or an unincorporate body, every director or manager of the corporate or unincorporate body is liable, upon conviction, as if the director or manager had personally committed the offence, unless the director or manager proves to the satisfaction of the court that the act constituting the offence was done without the knowledge, consent or connivance of the director or manager or that the director or manager took reasonable steps to prevent the commission of the offence.

FIRST SCHEDULE  
(Regulations 3,5,6,15 and 16)  
PRESCRIBED FORMS

Form I  
(Regulation 3)



THE FINANCIAL INTELLIGENCE CENTRE

The Financial Intelligence Centre Act, 2010

(Act No. 46 of 2010)

The Financial Intelligence Centre (General) Regulations, 2016

**DISSEMINATION AND PROVISION OF INFORMATION RELATED TO  
SUSPICIOUS TRANSACTIONS**

(Section 5 of the Financial Intelligence Centre Act, 2010)

Reference No.	
Your Reference (1)	
Name of the law enforcement agency	
<b>The information provided in this Form is for intelligence purposes only. This information should not be used or disseminated for evidential or judicial purposes and should not be disclosed to an unauthorised person without the prior written consent of the Financial Intelligence Centre.</b>	
Subject matter being disseminated/disclosed	
Total number of pages disseminated including this one	
If you did not receive the number of pages indicated, please contact the undersigned immediately.	

Signature.....

Name.....

Director

Date:.....



THE FINANCIAL INTELLIGENCE CENTRE

The Financial Intelligence Centre Act, 2010

(Act No. 46 of 2010)

**The Financial Intelligence Centre (General) Regulations, 2016**

REQUEST FOR INFORMATION

(Section 10 of the Financial Intelligence Centre Act, 2010)

Reference No.
To (Addressee):
Pursuant to section 5 of the Financial Intelligence Centre Act, 2010, you are requested to provide information according to the attached checklist in respect of the following person(s):Name:
<b>The information requested should be treated in strict confidentiality and should not be communicated directly or indirectly to any person involved in or assigned with the suspicious transaction or to an unauthorised third party.</b>
Information Required: 1. .... 2. ....
Frequency: ..... .....
Period to be covered by information: ..... .....

Signature:.....

Name.....

*Director*

Date í í í í í í í í í í í í í



THE FINANCIAL INTELLIGENCE CENTRE

The Financial Intelligence Centre Act, 2010  
(Act No. 46 of 2010)

**The Financial Intelligence Centre (General) Regulations, 2016**

FREEZING ORDER ( ) SUSPENSION ORDER ( )  
(Section 10 (2) of the Financial Intelligence Centre Act, 2010)

To (Addressee):

In accordance with section 10(2) of the Financial Intelligence Centre Act, 2010, you are directed to freeze the account/ suspend the transaction\* described below with immediate effect:

**Description of Account/Transaction\***

.....

.....

.....

.....

.....

.....

You are advised that failure to comply with this directive constitutes an offence contrary to section 10(3) of the Financial Intelligence Centre Act, 2010.

Signature:.....

Name.....

Director

Date í í í í í í í í í í í í í

\*Delete whichever is not applicable

Form IV  
(Regulation 6 (4))



THE FINANCIAL INTELLIGENCE CENTRE

The Financial Intelligence Centre Act, 2010  
(Act No. 46 of 2010)

**The Financial Intelligence Centre (General) Regulations, 2016**  
(Section 10 (2) of the Financial Intelligence Centre Act, 2010)

<p>To: (1).....</p> <p>.....</p> <p><b>REF: DISCHARGE OF FREEZING/SUSPENSION ORDER IN RESPECT OF (2)</b></p> <p>The freezing order number í í í í í í í í í í dated í í í í í í í í í í ..that was placed on this account/transaction has been lifted. Kindly allow the Account/ Transaction to operate normally.</p>
---

Dated this.....day of.....  
20.....

Signature:.....

Name:.....

Director

Notes:

1. Name of the reporting entity
2. Insert details of account/transaction



Form V  
(Regulation 15)



THE FINANCIAL INTELLIGENCE CENTRE  
The Financial Intelligence Centre Act, 2010  
(Act No. 46 of 2010)

**The Financial Intelligence Centre (General) Regulations, 2016**

**SUSPICIOUS TRANSACTION REPORT**

(Section 29 of the Financial Intelligence Centre Act, No. 46 of 2010)

**INSTRUCTIONS:**

1. Complete as much of this form as possible.
2. Fields marked with an asterisk (\*) are mandatory, except for attempted transactions.
3. Please complete form in INK and **CAPITAL LETTERS**.
4. Mark appropriate boxes with a cross (X).  
For further information on how to complete this form please refer to the STR Guidelines.
5. For electronic submission please log on to our *website at [www.fic.zm](http://www.fic.zm)*

**Send the Completed form to:**

The Director  
Financial Intelligence Centre  
P.O. Box 30481, Lusaka, Zambia  
or  
Email [FICSTR@fic.gov.zm](mailto:FICSTR@fic.gov.zm)

All Suspicious Transaction Reports (STRs) must, when completed, be treated as confidential.

**PART A: DETAILS OF THE PERSON/ORGANISATION TO WHICH THE SUSPICIOUS MATTER RELATES**

**1. .ACCOUNT OWNER(S)/HOLDER(S) – INDIVIDUAL**

1. Surname:
2. First Name:
3. Maiden Name:
4. Other Names:
5. Marital Status:
6. Date of Birth: (DD/MM/YYYY)    /    /
7. Sex: F     M
8. Profession:
9. Occupation:
10. Nationality:
11. Identity Type: National Registration Card     Passport     Driver's Licence 
  - (a) Identification Number:
  - (b) Date of issue:
  - (c) Place of Issue:
  - (d) Identification issued by:

**2. Residential Address\***

- (a) Property Number:
- (b) Street Name:
- (c) Area:
- (d) Village:
- (e) Chief:
- (f) District:
- (g) Province:
- (h) Country:

**3. Postal Address\*****4. Business Address**

- (a) Property Number:
- (b) Street Name:
- (c) Area:
- (d) District:
- (e) Province:

**5. Contact Details**

- (a) Telephone:
- (b) Mobile:
- (c) Fax:

If more than one person is involved, please provide the same details in this Part for each person, where appropriate, and attach.

## II. ACCOUNT OWNER(S)/HOLDER(S) - BUSINESS ENTITY

## 1. Name\*

2. Date of Registration\* (MM/DD/YYYY) / /

3. Registration Number\*

4. Country of Registration\*

5. Type of Business\*

- |   |  |
|---|--|
| (a) Company <input type="checkbox"/>        | (e) Sole trader <input type="checkbox"/> |
| (b) Partnership <input type="checkbox"/>    | (f) Cooperative <input type="checkbox"/> |
| (c) Statutory Body <input type="checkbox"/> | (g) Society <input type="checkbox"/>     |
| (d) Trust <input type="checkbox"/>          | (h) Other _____                          |

6. Nature of Business\*

7. Business Address (Head Office)

- (a) Property Number:
- (b) Street Name:
- (c) Area:
- (d) Village:
- (e) Chief:
- (f) District:
- (g) Province:
- (h) Country:

8. Postal Address\*

## 9. Contact details

- (a) Telephone:
- (b) Mobile:
- (c) Fax/Landline:
- (d) Email
- (e) Website

**PARTICULARS OF DIRECTORS/TRUSTEES/SETTLERS/BENEFICIARY**

- (a) Surname:
- (b) First Name:
- (c) Maiden Name:
- (d) Marital Status:
- (e) Nationality:
- (f) Occupation:
- (g) Identity Type and Number:
- (h) Date of issue:
- (i) Place of Issue:
- (j) Residential Address:

## Contact details

- (a) Mobile:
- (b) Landline:
- (c) Fax:
- (d) e-mail:

**PARTICULARS OF PERSON WITH AUTHORITY TO CONDUCT TRANSACTION ON BEHALF OF BUSINESS ENTITY/ TRUST**

- 12. Surname:
- 13. First Name:
- 14. Maiden Name:
- 15. Other Names:
- 16. Marital Status:
- 17. Date of Birth: (DD/MM/YYYY)     /     /
- 18. Sex: F      M
- 19. Profession:
- 20. Occupation:
- 21. Nationality:
- 22. Identity Type:    National Registration Card        Passport     Driver's Licence 
  - (e) Identification Number:
  - (f) Date of issue:
  - (g) Place of Issue:
  - (h) Identification issued by:

## Contact details

- (a) Mobile:
- (b) Landline:
- (c) Fax:
- (d) e-mail:

**PARTICULARS OF PERSON WITH AUTHORITY TO MANAGE, VARY OR CONTROL THE MANAGEMENT OF THE ENTITY/TRUST**

23. Surname: \_\_\_\_\_
24. First Name: \_\_\_\_\_
25. Maiden Name: \_\_\_\_\_
26. Other Names: \_\_\_\_\_
27. Marital Status: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_
28. Date of Birth: (DD/MM/YYYY) \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_
29. Sex: F M
30. Profession: \_\_\_\_\_
31. Occupation: \_\_\_\_\_
32. Nationality: \_\_\_\_\_
33. Identity Type: National Registration Card  Passport  Driver's Licence
- (i) Identification Number: \_\_\_\_\_
- (j) Date of issue: \_\_\_\_\_
- (k) Place of Issue: \_\_\_\_\_
- (l) Identification issued by: \_\_\_\_\_
- Contact details
- (a) Mobile: \_\_\_\_\_
- (b) Landline: \_\_\_\_\_
- (c) Fax: \_\_\_\_\_
- (d) e-mail: \_\_\_\_\_

**PART B:****ACCOUNT DETAILS**

25. Account Number* _____	33. Account/Product type* Accounting Services <input type="checkbox"/>	Trust <input type="checkbox"/>	Stored value card <input type="checkbox"/>
27. Branch/Office _____	Advisory Services <input type="checkbox"/>	Foreign Currency <input type="checkbox"/>	Superannuation <input type="checkbox"/>
28. Date account opened* DD/MM/YYYY- --/--/---	Auditing <input type="checkbox"/>	Insurance <input type="checkbox"/>	Trading <input type="checkbox"/>
29. Date account closed DD/MM/YYYY- --/--/---	Trading <input type="checkbox"/>	Investment <input type="checkbox"/>	Other <input type="checkbox"/>
	Betting <input type="checkbox"/>	Lease Hire/purchase <input type="checkbox"/>	
	Bullion <input type="checkbox"/>	Credit Facilities <input type="checkbox"/>	
	Demand/Cheque/Saving <input type="checkbox"/>	Conveyance of Property <input type="checkbox"/>	
	Credit/Debit Card <input type="checkbox"/>	Remittance <input type="checkbox"/>	
	Custodial <input type="checkbox"/>		
30. Other accounts held by this customer _____			
31. Details of person who closed account _____			
32. Status of account _____			

PART C: TRANSACTION DETAILS		
34. Purpose of transaction 35. parties to transaction 36. Place of transaction*..... 37. Date of Transaction__ __ *DD/MM/YYYY / / 38. Time of transaction HH:MM : 39. State period over which transaction conducted 40. Total amount of transaction (ZMK)*..... 41. Assets involved, Currency Amount, value and type (Specify)..... 42. Method of transaction..... 43. Method of disposal of funds or property..... 44. Amount of disposition of funds or assets.....	45. Transaction Type* Account Opening <input type="checkbox"/> Account Depositing <input type="checkbox"/> Account Withdrawal <input type="checkbox"/> Traveller's cheques <input type="checkbox"/> Funds Transfer <input type="checkbox"/> Transfer of Property <input type="checkbox"/>	46. Purchase of Negotiable Instrument <input type="checkbox"/> Disposal of Instruments <input type="checkbox"/> Contribution <input type="checkbox"/> Premium <input type="checkbox"/> Bet Placed <input type="checkbox"/> Remittance <input type="checkbox"/>
47. Any previous activity in the preceding 180 days which had been considered for reporting in connection with the account, whether the activity was reported or not. 48. The report number of any previous reports made in connection with the account	Other (Specify).....	
PART D: CATEGORY FOR SUSPICION		
REASON FOR SUSPICION (Tick at least one)		

- |   |                          |                                     |                          |
|---|--------------------------|-------------------------------------|--------------------------|
| Person - Suspicious Behaviour                       | <input type="checkbox"/> | ATM fraud                           | <input type="checkbox"/> |
| Irregular or unusual international banking activity | <input type="checkbox"/> | Advance fee Scam                    | <input type="checkbox"/> |
| Large or unusual cash deposit                       | <input type="checkbox"/> | Large or unusual cash withdrawals   | <input type="checkbox"/> |
| Activity inconsistent with customer profile         | <input type="checkbox"/> | Corporate/Investment fraud          | <input type="checkbox"/> |
| Large or unusual inward remittance                  | <input type="checkbox"/> | Large or unusual outward remittance | <input type="checkbox"/> |
| Unusually large foreign currency transaction        | <input type="checkbox"/> | Credit Card fraud                   | <input type="checkbox"/> |
| Country/jurisdiction risk                           | <input type="checkbox"/> | Credit/loan facility fraud          | <input type="checkbox"/> |
| False name/identity                                 | <input type="checkbox"/> | Currency not declared at border     | <input type="checkbox"/> |
| Counterfeit currency                                | <input type="checkbox"/> | Immigration related issue           | <input type="checkbox"/> |
| Fraud   | <input type="checkbox"/> | Internet fraud                      | <input type="checkbox"/> |
| Avoiding reporting obligations                      | <input type="checkbox"/> | National Security concern           | <input type="checkbox"/> |
| Known/suspected criminal/organization               | <input type="checkbox"/> | Unauthorised Transaction            | <input type="checkbox"/> |

Unusual business practices	<input type="checkbox"/>	Unusual Financial Instrument	<input type="checkbox"/>
Many third parties making deposits into the account	<input type="checkbox"/>	Unusual Gambling	<input type="checkbox"/>
Watch listed individual/organization	<input type="checkbox"/>	Other (Specify): _____	
Phishing (Electronic Fraud)	<input type="checkbox"/>	(Attach extra leaf if necessary)	
Or inactive account	<input type="checkbox"/>		

#### DESCRIPTION OF TRANSACTION

##### Transaction Narrative\*

Please describe clearly and completely the factors or unusual circumstances that led to the suspicion. Further, indicate whether the transaction is an isolated incident or involves other transactions. Provide as much details as possible to explain what was suspicious. Has this matter been reported to any Law Enforcement Agency, if yes, please specify. If there is insufficient space, a

Indicate what action the natural or legal person making the report, or other entity on whose behalf the report is made, has taken in connection with the transaction concerning which the report is made.

Indicate what documentary proof, if any, is available in respect of the transaction concerning which the report is made.

#### PART E: REPORTING ENTITY DETAILS\*

**NATURE OF BUSINESS**

Micro Finance Institution	<input type="checkbox"/>	Lotteries	<input type="checkbox"/>	Motor Vehicle Dealer	<input type="checkbox"/>	Precious metal Dealer	<input type="checkbox"/>
Leasing Company	<input type="checkbox"/>	Real Estate Agent	<input type="checkbox"/>	Legal Practitioner	<input type="checkbox"/>	Insurance	<input type="checkbox"/>
Building Society	<input type="checkbox"/>	Real Estate Dev.	<input type="checkbox"/>	Accountant/Auditor	<input type="checkbox"/>	Pension	<input type="checkbox"/>
Commercial Bank	<input type="checkbox"/>	Stock Broker	<input type="checkbox"/>	Tax Consultant	<input type="checkbox"/>	Development Finance	<input type="checkbox"/>

Other (Specify) \_\_\_\_\_

Reporting Entity Name\* \_\_\_\_\_

Physical Address \_\_\_\_\_

**Compliance/Reporting Officer**

Name \_\_\_\_\_

Position \_\_\_\_\_

Tel No: \_\_\_\_\_

Landline: +260	Mobile: +260
Fax: +260	Email Address:

**If different from Compliance /Reporting Officer**

Name \_\_\_\_\_

Position \_\_\_\_\_

Tel No: \_\_\_\_\_

Landline: +260	Mobile: +260
Fax: +260	Email Address:

Are there any attachments accompanying this form?    Yes     No

(If yes, please specify): \_\_\_\_\_

Date: MM/DD/YYYY \_\_\_/\_\_\_/\_\_\_\_\_

.....  
Signature

.....  
Reporting Officer Signature\*

**Please submit completed STR to FIC not later than three working days of forming the suspicion**

<p><b>FOR OFFICIAL USE ONLY</b></p> <p><b>STR NO:</b></p> <p><b>DATE RECEIVED:</b></p> <p><b>NAME:</b></p>    <p>(Signature) _____</p> <p style="text-align: center;"><i>Authorised Officer</i></p>
---





THE FINANCIAL INTELLIGENCE CENTRE

**The Financial Intelligence Centre Act, 2010**

(Act No. 46 of 2010)

The Financial Intelligence Centre (General) Regulations, 2016

**OATH/AFFIRMATION**

I ....., do swear/affirm that I will be faithful and bear allegiance to the President of the Republic of Zambia, and that I will preserve, protect and defend the Constitution of Zambia, as by law established.

SO HELP ME GOD.

.....  
(Signature)

Sworn at ..... this ..... day of ....., 20.....  
Before me,

.....  
*President*

SECOND SCHEDULE  
(Regulations 9 and 10)

RISK FACTORS

PART I

A. A reporting entity shall take into account the following risk factors where the reporting entity determines that the risk of money laundering or terrorist financing is low:

1. Customer risk factors

- (a) a customer is subject to requirements to combat money laundering and terrorist financing consistent with the provisions of the Act, has effectively implemented those requirements, and is effectively supervised or monitored in accordance with the Act to ensure compliance with those requirements;
- (b) a customer is a public company listed on a stock exchange and subject to disclosure requirements through law or other enforceable means, which impose requirements to ensure adequate transparency of beneficial ownership; and
- (c) a customer is a State enterprise, local authority or statutory body.

2. Product, service, transaction or delivery channel risk factors

- (a) a financial product or service that provides appropriately defined and limited services to certain type of customers so as to increase access for financial inclusion purposes;
- (b) a life insurance policy where the annual premium is not more than five thousand Kwacha (ZMW5,000.00) or a single premium of not more than thirteen thousand Kwacha (ZMW13,000.00) or such other higher amount determined by the Centre;
- (c) a pension, superannuation or similar scheme providing retirement benefits to employees, where contributions are made by way of deduction from the wages or salaries and where the rules of such scheme do not permit assignment of member's interest under the scheme;
- (d) an insurance policy for a pension scheme where there is no surrender clause and the policy cannot be used as collateral;
- (e) benefits of a product or related transaction which cannot be realised for the benefit of a third party except in the case of death, disablement, survival to a pre-determined advanced age or other event; and
- (f) a product of which during the contractual relationship, no accelerated payments are made, or surrender clauses or early termination takes place.

3. Country risk factors

- (a) a country identified by sources such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems; and
- (b) a country identified by credible sources as having a low level of corruption or other criminal activity.

## PART II

B. A reporting entity shall take into account the following risk factors where the risk of money laundering or terrorist financing may be high:

1. Customer risk factors:

- (a) the business relationship is conducted in unusual circumstances such as significant unexplained geographic distance between the financial institution and the customer;
- (b) non-resident customers;
- (c) legal persons or arrangements that are personal asset-holding vehicles;
- (d) companies that have nominee shareholders or shares in bearer form;
- (e) business that are cash-intensive; and
- (f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

2. Country or geographic risk factors:

- (a) countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate systems for combating money laundering or terrorist financing;
- (b) countries subject to sanctions, embargos or similar measures issued by the United Nations or similar international organisation;
- (c) countries identified by credible sources as having significant levels of corruption or other criminal activity; and
- (d) countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

3. Product, service, transaction or delivery channel risk factors:

- (a) private banking;
- (b) anonymous transactions, which may include cash;
- (c) non-face-to-face business relationships or transactions; and
- (d) payment received from unknown or un-associated third parties.

LUSAKA

22nd January, 2015

[MF/IDM/52/2/7SEC]

A.B. CHIKWANDA,  
*Minister of Finance*

