GOVERNMENT OF ZAMBIA

STATUTORY INSTRUMENT NO. 54 OF 2022

The Financial Intelligence Centre Act, 2010
(Act No. 46 of 2020)

The Financial Intelligence Centre (General) Regulations, 2022

ARRANGEMENT OF REGULATIONS

Regulation

Copies of this Statutory Instrument can be obtained from the Government Printer, P.O. Box 30136, 10101, Lusaka, Price K80.00 each

IN EXERCISE of the powers contained in section 58 of the Financial Intelligence Centre Act, 2010, and in consultation with the Centre, the following Regulations are made:

PART I
PRELIMINARY

Title

1. These Regulations may be cited as the Financial Intelligence Centre (General) Regulations, 2022.

Interpretation

2. (1) In these Regulations, unless the context otherwise requires—

"account" has the meaning assigned to the word in the Act;

"accountable institution" has the meaning assigned to the words in the Act;

"beneficiary", in relation to a non-governmental organisation, means the person who receives a benefit, either directly or indirectly, for a charitable, religious, cultural, educational, political, social, fraternal or philanthropic purpose and, includes both the ultimate beneficiary and any intermediaries;

"beneficial owner" has the meaning assigned to the words in the Act;

"Centre" has the meaning assigned to the word in the Act;

"citizen" has the meaning assigned to the word in the Constitution; Cap.1

"competent authority" has the meaning assigned to the words in the Act;

"council" has the meaning assigned to the word in the Constitution; Cap.1

"designated nonfinancial business or profession" has the meaning assigned to the words in the Act;

"director" has the meaning assigned to the word in the Act;

"Director-General" means the Director-General of the Financial Intelligence Centre appointed under the Act;

"Egmont Group" means the international network of financial intelligence units established to promote and enhance international cooperation and information sharing among financial intelligence units relating to the fight against money laundering or financing of terrorism or proliferation or any other serious offence relating to money laundering, financing of terrorism or proliferation;

"financial service provider" has the meaning assigned to the words in the Act;

"foreign designated authority" has the meaning assigned to the words in the Act;

Act No. 16 of 2009

"intermediary institution" has the meaning assigned to the words in the Act;

"law enforcement agency" has the meaning assigned to the words in the Act;

"non- governmental organisation" has the meaning assigned to the words in the Non-Governmental Organisations Act, 2009;

Act No. 16 of 2009

"political party" has the meaning assigned to the words in the Constitution;

Cap. 1

"public function" has the meaning assigned to the words in the Act;

"public office" has the meaning assigned to the words in the Act;

"proliferation financing" has the meaning assigned to the words in the AntiTerrorism and Non- Proliferation Act, 2018;

Act No. 6 of 2018

"Registrar of Companies" means the person appointed as Registrar under the Patents and Companies Registration Agency Act, 2020;

Act No. 4 of 2020

"reporting entity" has the meaning assigned to the words in the Act;

"supervisory authority" has the meaning assigned to the words in the Act;

"suspicious transaction report" has the meaning assigned to the words in the Act;

"transaction" has the meaning assigned to the word in the Act; and "Zambia Revenue Authority" means the Zambia Revenue Authority established under the Zambia Revenue Authority Act.

Cap. 321

PART II
Access And Dissemination Of Information

Dissemination and disclosure of suspicious transactions

3. The Centre shall disseminate and provide information, following its analysis of suspicious transactions, to a law enforcement agency and a foreign designated authority for purposes of the Act in Form I set out in the First Schedule.

Access to information

4. The Centre may, in exercising its functions under the Act and these Regulations, use electronic communication services to access, directly or indirectly, on a timely basis, financial, administrative and law enforcement information.

Request for information

5. The Director-General shall request a reporting entity to provide financial information, in Form II set out in the First Schedule.

Freezing account and suspending transaction

6. (1) The Director-General shall order a reporting entity to freeze an account or suspend a transaction in Form III set out in the First Schedule.

(2) The Centre shall serve a signed copy of a freezing or suspension order under subregulation (1) on a reporting entity where the account is held, or the transaction is processed or intended to be processed.

(3) A reporting entity shall, on receipt of the freezing or suspension order issued under subregulation (1)—

(a) stop all activity on the account concerned with the exception of credits received into that account; and

(b) suspend the specified transaction for the duration specified in the order.

(4) An order issued under this regulation shall remain in operation until—

(a) the expiration of the period of fifteen days from the date of its issuance; or

(b) a judge, on aplication by a person aggrieved with the decision of the Director-General, issues an order discharging the freezing order issued by the Director-General.

(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 order and as at 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 a natural person, the reporting entity shall verify the full name and physical address, and date and place of birth or a mobile number linked to a registered international mobile equipment identity number or sim card in place of a physical address by comparing these particulars with—

(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, a professional, customary authority or an existing customer of a reporting entity 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 non-resident or non-citizen;

(iv) a Refugee Identification Card, in the case of a natural person with a refugee status;

(v) information obtained through a credit reference agency search;

(vi) an original or certified true copy of the latest council or applicable rates or utility bill receipt;

(vii) 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; or

(viii) a permit allowing a customer to reside in the Republic in addition to the information required under subregulation (1)(a)(i) to (vi), in the case of a customer who is a citizen of another country;

(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 issued by the Zambia Revenue Authority and other information contained in the Register of companies or other relevant register; and

(iii) except for statutory bodies, by verifying particulars of every person exercising direct or indirect control, for purposes of identifying the beneficial owner; and

(c) for a partnership, obtain from an individual acting or purporting to act on its behalf the—

(i) name of the partnership;

(ii) business address;

(iii) partnership agreement; and

(iv) 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 under subregulation (1) apply to an individual acting on behalf of the customer in establishing an account or a business relationship with a reporting entity.

(3) A reporting entity shall, where the legal arrangement is a trust, verify the particulars obtained in respect of the trust by comparing the name of the trustee, the settler, beneficiary and any other natural person exercising ultimate effective control over the trust, with the trust deed or other founding document in terms of which the trust is created.

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

(5) A reporting entity shall, 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 a legal arrangement, in addition to the other steps as may be applicable under subregulation (1), obtain from the individual a power-of-attorney, a 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 documents, data or information periodically in order to ensure that the verification process provides accurate information for purposes of the Act and these Regulations.

(7) An update referred to under subregulation (6) shall be occasioned by a change in—

(a) the authorised signatories;

(b) the purpose of account or business relationship;

(c) the scope of terms and conditions applicable to the account or customer profile;

(d) declared income and actual account or business transaction activity;

(e) the nature of business;

(f) business operational address;

(g) customer address details;

(h) customer contact details;

(i) shareholding structure;

(j) management or board structure; or

(k) any other material aspects of, or likely to affect, an account.

Risk-based application of customer due diligence

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, terrorism or proliferation financing risk associated with the products, services, delivery channels, customer, geographical location, country risk, business relationship or transaction.

Low risk of money laundering, terrorism or proliferation financing

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

(2) A reporting entity may, in applying simplified customer due diligence measures—

(a) verify the identity of the customer and the beneficial owner after the establishment of the business relationship;

(b) reduce the frequency of customer identification updates;

(c) reduce the degree of ongoing monitoring and scrutinising of transactions; and

(d) infer the purpose and nature from the type of transaction or business relationship established and not collect specific information or carry out specific measures to understand the purpose and intended nature of the business relationship .

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

(4) Simplified measures undertaken under this regulation shall be commensurate with the lower risk factors.

(5) Simplified measures shall not be applied where there is a suspicion of money laundering, terrorism or proliferation financing, or where there is a specific higher risk scenario of money laundering, terrorism or proliferation financing.

(6) 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.

High risk of money laundering or terrorism or proliferation financing

10. (1) A reporting entity shall apply enhanced identification, verification and ongoing due diligence measures in circumstances 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, terrorism or proliferation financing to be high.

(2) Enhanced due diligence measures taken by a reporting entity under subregulation (1) shall include—

(a) examining the background and purpose of a transaction; and

(b) increasing the degree and nature of monitoring of business relationships made, to determine whether the transaction or business relationship is suspicious.

Reliance on identification by third party

11. (1) A reporting entity may rely on a third party to perform customer identification where that third party is established in, or subject to, the jurisdiction of the States that—

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

(b) are not subject to monitoring by the Financial Action Task Force's International Cooperation Review Group or Regional Review Group; or

(c) are not subject to United Nations sanctions or other applicable sanctions.

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

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

(b) third party's

(i) full name, if the third party is a natural person; or

(ii) registered name, if the third party is a company;

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

(d) 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 obligation of due diligence;

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

(f) full name and contact particulars of the individual who liaises with the third party on behalf of the reporting entity concerning the retention of that 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 obligation of due diligence for at least ten years from the end of the business relationship between the reporting entity and its customer.

PART IV

MEASURES RELATING TO A NON-GOVERNMENTAL ORGANISATION AND OBLIGATIONS FOR AN ACCOUNTABLE INSTITUTION

Monitoring of non-governmental organisation by competent authority

12. (1) A competent authority shall rely on the measures set out in the Third Schedule to monitor compliance by a non-governmental organisation for purposes of enforcing compliance for preventing or combating terrorist financing abuse of a non-governmental organisation.

(2) The measures under subregulation (1) apply to a non-governmental organisation that primarily engages in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works.

Obligations of accountable institutions

13. An accountable institution is subject to the obligations set out in the Fourth Schedule.

PART V
RISK MANAGEMENT

Risk management systems

14. A reporting entity shall implement risk management systems to identify high risk customers whose activities may pose a high risk of money laundering, terrorism or proliferation financing 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) geographic location of the customer or transaction;

(iv) the magnitude of customer assets that a reporting entity handles;

(v) third parties that may be involved in the customer's activities;

(vi) the beneficial ownership of an entity and their impact on risk;

(vii) the volume of cash used by a customer in transactions; and

(viii) any other indicators 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.

Internal programmes to combat money laundering, terrorism or proliferation financing and any other serious offence

15. The type and extent of measures that a reporting entity shall undertake for the prevention of money laundering, terrorism or proliferation financing and any other serious offence relating to money laundering, terrorism or proliferation financing that is risk based includes—

(a) identifying the money laundering, terrorism or proliferation 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)*;

(f) establishing and implementing 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; and

(g) identifying and handling wire transfers that are not accompanied by complete originator information by obtaining and verifying missing information from the ordering institution or the beneficiary in relation to a wire transfer on the basis of the risk associated with the transaction.

Measures for business relations and transactions emanating from countries that insufficiently comply with international standards

16. (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, terrorism or proliferation financing and any other serious offence relating to money laundering, terrorism or proliferation financing—

(a) take into account risks arising from the deficiencies in the regime for combating money laundering, terrorism or proliferation financing and any other serious offence relating to money laundering, terrorism or proliferation financing in any given country;

(b) consider publicly available information for identifying countries which do not, or insufficiently, apply the relevant international standards to combat money laundering, terrorism or proliferation financing and any other serious offence relating to money laundering, terrorism or proliferation financing; and

(c) examine the background and purpose of the transaction.

(2) A reporting entity shall, if a transaction has no apparent economic or lawful purpose—

(a) examine the background and purpose of the transaction;

(b) record the findings and retain the record of transaction; and

(c) submit, on request, to the Centre, a supervisory authority or law enforcement agency the record referred to under paragraph *(b)*.

PART VII
General Provisions

Reporting suspicious transactions

17. (1) A report of a suspicious transaction by a financial service provider and for a designated non-financial business or profession shall be in Form IV and Form V, respectfully, 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 the Centre.

(2) A report referred to under subregulation (1) shall contain a full description of the suspicious transaction and state the reason why it is considered suspicious.

Compliance order

18. The Director-General shall, for the purposes of section 37C of the Act, serve a compliance order in Form VI set out in the First Schedule.

Certificate of appointment and identity card of inspector

19. The Director-General shall issue an inspector appointed under section 11A of the Act with—

(a) a certificate of appointment in Form VII set out in the First Schedule; and

(b) an identity Card in Form VIII set out in the First Schedule.

Reporting entity to be registered or licensed

20. (1) A reporting entity shall be registered or licensed by a designated supervisory authority for the purposes of the Centre supervising and enforcing compliance under the Act and these Regulations.

(2) A virtual asset service provider shall, where the reporting entity is a virtual asset service provider that is a legal person, be registered or licensed in the jurisdiction where the virtual asset service provider is created.

(3) Where the reporting entity is a virtual asset service provider that is a natural person, the virtual asset service provider shall be registered or licensed in the jurisdiction where the place of business of the virtual asset service provider is located.

(4) A person who contravenes this regulation is liable to an administrative sanction provided under the Act.

Oath and affirmation

21. The Director-General shall administer oaths or affirmations in Form IX set out in the First Schedule.

General Penalty

22. A person who contravenes any provision of these Regulations which is not an offence and for which a sanction is not provided is liable to an administrative sanction provided under the Act.

Contravention by principal officer of body corporate or unincorporate body

23. Where a contravention under these Regulations is committed by a body corporate or unincorporate body, with the knowledge, consent or connivance of the director, manager, shareholder or partner of the body corporate or unincorporate body, that director, manager, shareholder or partner is liable to an administrative sanction provided under the Act.

Revocation of S.I No. 9 of 2016

24. The Financial Intelligence Centre (General) Regulations, 2016, are revoked.

FIRST SCHEDULE
(Regulations 3, 5, 6, 17, 18, 19 and 21)

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, 2022

DISSEMINATION AND DISCLOSURE OF SUSPICIOUS TRANSACTIONS

Reference No.	
Your Reference (1)	
Name of the law enforcement agency	
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.	
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.	

Name ……

Signature ……

Director-General

Date: ……..

FORM II
(Regulation 5)

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

REQUEST FOR INFORMATION

Reference No.
To (Addressee):
Pursuant to section 10 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:
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.
Information Required: 1. …… 2. …… Frequency: …… Period to be covered by information: ……

Signature:……

Name…….
Director-General

Date……

FORM III
(Regulation 6(1))

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

FREEZING ORDER ( ) SUSPENSION ORDER ( )

To (Addressee):
In accordance with section 10(3) 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(5) and (6) of the Financial Intelligence Centre Act, 2010.

Signature:…….

Name……..
Director-General

Date……

***Delete whichever is not applicable**

FORM IV
(Regulation 17(1))

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

SUSPICIOUS TRANSACTION REPORT
FINANCIAL SERVICE PROVIDER

INSTRUCTIONS:

1. Complete as much of this Form as possible in **CAPITAL LETTERS**..
2. Fields marked with an asterisk (*) are mandatory, except for attempted transactions.
3. Mark appropriate boxes with a cross (X).
   For further information on how to complete this Form please refer to the sector specific STR Guidelines which are available on our website at www.fic.gov.zm.

Send the Completed form to:

Via the **Online Portal**
In exceptional circumstances send the completed form via email to :
FICSTR@fic.gov.zm
or to
The Director General
Financial Intelligence Centre
P.O. Box 30481, Lusaka, Zambia

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

I. CLIENT INFORMATION –INDIVIDUAL

1. Surname:
2. First Name:
3. Middle Name:
4. If known by another Name - Specify:
5. Nationality:
6. Country of origin:
7. Date of Birth: (DD/MM/YYYY) / /
8. Sex: F ☐ M ☐
9. Profession:
10. Occupation:
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:

12. Residential Address*
    (a) Property Number:
    (b) Street Name:
    (c) Residential Area:
    (d) Village:
    (e) Chief:
    (f) City:
    (g) Town:
    (h) District:
    (i) Province:
    (j) Country:

13. Postal Address*

14. Contact Details
    (a) Telephone:
    (b) Mobile:
    (c) Email:

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

II. CLIENT INFORMATION - BUSINESS ENTITY

15. Name*
16. Date of Registration* (MM/DD/YYYY) / /
17. Registration Number*
18. Country of Registration*
19. Tax Payer Identification Number (TPIN)*
20. Type of Business*

(a) Company		*(f)* Sole trader	
(b) Partnership		*(g)* Cooperative	
(c) Statutory Body		*(h)* Society	
(d) NGO		*(i)* Trust	
(e) Other			

21. Nature of Business*
22. Physical Address
    (a) Property Number:
    (b) Street Name:
    (c) Area:
    (d) Village:
    (e) Chief:
    (f) City:
    (g) Town:

(h) District:
(i) Province:
(j) Country:

23. Postal Address*

24. Contact details
(a) Telephone:
(b) Mobile:
(c) Email:
(d) Company Website:

25. **PARTICULARS OF COMPANY HEAD**
(a) Surname:
(b) First Name:
(c) Middle Name:
(d) Nationality:
(e) Country of Origin:
(f) Occupation:
(g) Identity Type: National Registration Card ☐ Passport ☐ Driver's Licence ☐
(h) Identification Number*:
(i) Date of issue:
(j) Place of Issue:
(k) Contact details:
(a) Mobile:
(b) Landline:
(c) Email:

III: ACCOUNT/PRODUCT DETAILS			
26. Account Number/Unique Identifier Number* _____ 27. Date Account/Relationship Established* DD/MM/YYYY- ___/___/_____ 28. Other accounts held by this customer_____	29. Account/Product type* Advisory Services ☐ Trading ☐ Bullion ☐ Demand/Cheque/Saving ☐ Credit/Debit Card ☐ Custodial ☐	Foreign Currency ☐ Insurance ☐ Investment ☐ Invoice Discounting ☐ Credit Facilities ☐ Remittance ☐	Stored value card ☐ Leasing ☐ Letter of Credit ☐ Superannuation ☐ Virtual Asset Services ☐ Other ☐

PART B: TRANSACTION DETAILS

30. Place of transaction*……	35. Transaction Type*	
31. Date of Transaction*DD/MM/YYYY---- ___/___/_____	Account Opening ☐	Purchase of ☐
32. Time of transaction HH:MM ___:___	Account Depositing ☐	Negotiable Instrument ☐
33. Total amount of transaction (ZMW)* …… ……	Account Withdrawal ☐	Disposal of Instruments ☐
34. Foreign Currency Amount and Type (Specify) …..……	Traveller's cheques ☐	Contribution ☐
	Funds Transfer ☐	Premium ☐
	Transfer of Property ☐	Bet Placed ☐
	Remittance ☐	Other (Specify): ☐

PART C: CATEGORY FOR SUSPICION

I. REASON FOR SUSPICION (Tick at least one)

36. Indicate the reason for suspicion

Person – Suspicious Behaviour	☐	ATM fraud	☐
Irregular or unusual international banking activity	☐	Advance fee Scam	☐
Large or unusual cash deposit	☐	Large or unusual cash withdrawals	☐
Activity inconsistent with customer profile	☐	Corporate/Investment fraud	☐
Large or unusual inward remittance	☐	Large or unusual outward remittance	☐
Unusually large foreign currency transaction	☐	Credit Card fraud	☐
Country/jurisdiction risk	☐	Credit/loan facility fraud	☐
False name/identity/documents	☐	Currency not declared at border	☐
Counterfeit currency	☐	Immigration related issue	☐
Fraud	☐	Internet fraud	☐
Avoiding reporting obligations	☐	National Scurity concern	☐
Known/suspected criminal/organization	☐	Unauthorised Transaction	☐
Unusual business practices	☐	Unusual Financial Instrument	☐
Many third parties making deposits into the account	☐	Unusual Gambling	☐
Watch listed individual/organization	☐	Other (Specify): _____	
Phishing (Electronic Fraud)	☐	(Attach extra leaf if necessary)	
Or inactive account	☐		

II. 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 and provide details of other entities or persons involved in the transaction. 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, attach a separate statement.

PART D: REPORTING ENTITY DETAILS*

NATURE OF BUSINESS

Micro Finance Institution ☐ Insurance Broker ☐ Lotteries ☐ Money Remitter ☐ Stock Broker ☐

Leasing Company ☐ Bureau de Change ☐ Building Society ☐ Commercial Bank ☐ Insurance ☐

Development Finance ☐ Pension ☐ Other (Specify) _____

Reporting Entity Name* _____

Physical Address _____

Compliance/Reporting Offic

Name _____

Position _____

Tel No:

Landline: +260	Mobile: +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

FOR OFFICIAL USE ONLY

STR NO:
DATE RECEIVED:
NAME:

(Signature) _____

Authorised Officer

FORM V
(Regulation 17(1))

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

SUSPICIOUS TRANSACTION REPORT
DESIGNATED NON-FINANCIAL BUSINESS OR PROFESSION

INSTRUCTIONS:

1. Complete as much of this Form as possible in **CAPITAL LETTERS**..
2. Fields marked with an asterisk (*) are mandatory, except for attempted transactions.
3. Mark appropriate boxes with a cross (X).
   For further information on how to complete this Form please refer to the sector specific STR Guidelines which are available on our website at www.fic.gov.zm.

Send the Completed form to:

Via the **Online Portal**
In exceptional circumstances send the completed form via email to :
FICSTR@fic.gov.zm
or to
The Director General
Financial Intelligence Centre
P.O. Box 30481, Lusaka, Zambia

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

I. CLIENT INFORMATION –INDIVIDUAL

1. Surname:
2. First Name:
3. Middle Name:
4. If known by another Name - Specify:
5. Nationality:
6. Country of origin:
7. Date of Birth: (DD/MM/YYYY) / /
8. Sex: F ☐ M ☐
9. Profession:
10. Occupation:
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:

12. Residential Address*
    - *(a)* Property Number:
    - *(b)* Street Name:
    - *(c)* Residential Area:
    - *(d)* Village:
    - *(e)* Chief:
    - *(f)* City:
    - *(g)* Town:
    - *(h)* District:
    - *(i)* Province:
    - *(j)* Country:

13. Postal Address*

14. Contact Details
    - *(a)* Telephone:
    - *(b)* Mobile:
    - *(c)* Email:

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

II. CLIENT INFORMATION - BUSINESS ENTITY

15. Name*
16. Date of Registration* (MM/DD/YYYY) / /
17. Registration Number*
18. Country of Registration*
19. Tax Payer Identification Number (TPIN)*
20. Type of Business*

(a) Company		*(f)* Sole trader	
(b) Partnership		*(g)* Cooperative	
(c) Statutory Body		*(h)* Society	
(d) NGO		*(i)* Trust	
(e) Other			

21. Nature of Business*
22. Physical Address
    - *(a)* Property Number:
    - *(b)* Street Name:
        - *(a)* Area:
        - *(b)* Village:
        - *(c)* Chief:
    - *(d)* City:
    - *(e)* Town:
    - *(f)* District:

(g) Province:
(h) Country:
23. Postal Address*
24. Contact details
(a) Telephone:
(b) Mobile:
(c) Email:
(d) Company Website:

25. **PARTICULARS OF COMPANY HEAD**
(a) Surname:
(b) First Name:
(c) Middle Name:
(d) Nationality:
(e) Country of Origin:
(f) Occupation:
(g) Identity Type: National Registration Card ☐ Passport ☐ Driver's Licence ☐
(h) Identification Number*:
(i) Date of issue:
(j) Place of Issue:
(k) Contact details:
(a) Mobile:
(b) Landline:
(c) Email:

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

III: ACCOUNT/PRODUCT DETAILS		
26. Account Number/Unique Identifier Number* _____ 27. Date Account/Relationship Established* DD/MM/YYYY- ___/___/_____	28. Account/Product type* Accounting Services ☐ Advisory Services ☐ Auditing ☐ Lease/Hire ☐ Consulting Services ☐ Betting/Gaming ☐	Trust and Company Services ☐ Managing of Client Assets ☐ Precious stone trading ☐ Precious metals trading ☐ Buying & selling of Property ☐ Conveyance of Property ☐ Other (Specify):_____

PART B: TRANSACTION DETAILS

29. Place of transaction*……	34. Transaction Type*
30. Date of Transaction*DD/MM/YYYY---- ___/___/_____	Cash Payment ☐
31. Time of transaction HH:MM ___:___	Funds Transfer ☐
32. Total amount of transaction (ZMW)* ……	Property Swap ☐ Cheque Payment ☐ Cashing of Chips ☐
33. Foreign Currency Amount and Type (Specify) …..……..	Attempted Transaction ☐ Other (Specify): _____

PART C: CATEGORY FOR SUSPICION

I. REASON FOR SUSPICION (Tick at least one)

35. Indicate the reason for suspicion

Person – Suspicious Behaviour	☐	Unusual business practices	☐
Large or unusual cash transaction	☐	Advance fee Scam	☐
Activity inconsistent with customer profile	☐	Unusual Gambling	☐
Large or unusual inward remittance	☐	Large or unusual outward remittance	☐
Unusually large foreign currency transaction	☐	Country/jurisdiction risk	☐
False name/identity/documentation	☐	Phishing (Electronic Fraud)	☐
Counterfeit currency	☐	Immigration related issue	☐
Fraud	☐	Internet fraud	☐
Avoiding reporting obligations	☐	National Security concern	☐
Known/suspected criminal/organization	☐	Unauthorised Transaction	☐
Watch listed individual/organization	☐	Other (Specify): _____	

II. 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 and provide details of other entities or persons involved in the transaction. 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, attach a separate statement.

PART D: REPORTING ENTITY DETAILS*

NATURE OF BUSINESS

Motor Vehicle Dealer ☐ Precious stone/metal Dealer ☐ Tax Consultant ☐ Casino ☐
Leasing Company ☐ Real Estate Agency ☐ Legal Practitioner ☐ Betting ☐
Accountant/Auditor ☐ Real Estate Development ☐ Other (Specify) _____

Reporting Entity Name* _____
Physical Address _____

Compliance/Reporting Officer

Name _____
Position _____
Tel No:

Landline: +260	Mobile: +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

FOR OFFICIAL USE ONLY

STR NO:
DATE RECEIVED:
NAME:

(Signature) _____
Authorised Officer

FORM VI
(Regulation 18
(To be Completed in duplicate))

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

COMPLIANCE ORDER

To: The Executive Director

(1) Here state the name of reporting entity to which Compliance Order is issued

…..……. (1)

Address: …… (2)

(2) Here insert address of reporting entity to which Compliance Order is Issued

TAKE NOTICE that the Financial Intelligence Centre has issued this Compliance Order based on the following grounds (3):

(a) ……

(b) ……

(c) ……

(d) ……

(3) Here state the grounds on which the Compliance Order is being issued

TAKE NOTICE that you are required to undertake the following action within the stipulated time frame (4):

(a) ……

(b) ……

(c) ……

(4) Here state the action to be undertaken and the time frame for each action

TAKE NOTICE that failure to comply with this directive constitutes an offence contrary to section 37C(3), (5) and (6) of the Financial Intelligence Centre Act, 2010.

Signature:……..

Name……..
Director-General

Date……

FORM VII
(Regulation 19(a)
(To be Completed in duplicate)

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

CERTIFICATE OF APPOINTMENT AS INSPECTOR

(1) Here insert full names of inspector
(2) Here insert address of inspector
(3) Here insert period of appointment

TAKE NOTICE that (1) …… of (2) …….. has been appointed as an inspector by the Financial Intelligence Centre for a term of (3) …… and has authority to perform the following functions as directed by the Financial Intelligence Centre pursuant to section 11B of the Financial Intelligence Centre Act, 2010:

(a) ……

(b) ……

(c) ……

(d) ……

Signature:…….

Name……..
Director-General

Date……

FORM VIII
(Regulation 19(B)
(To be Completed in duplicate)

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

INSPECTOR IDENTIFICATION CARD

(1) Here insert full names of inspector
(2) Here insert inspector's picture
(3) Here insert designation
(4) Here insert card number
(5) Here insert period of appointment

Full Name

(1):……

(2) Insert Picture

Designation (3): ….……

Card Number (4): ……

Period of Appointment (5): …….

Signature:…….

Name……..
Director-General

Date…….

FORM IX
(Regulation 21)

The Financial Intelligence Centre

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

The Financial Intelligence Centre (General) Regulations, 2022

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 risk factors specified in this Part where the reporting entity determines that the risk of money laundering or terrorism or proliferation financing is low.

1. Customer risk factors include—

(a) a customer is subject to requirements to combat money laundering and terrorism or proliferation 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;

(d) a customer whose monthly income does not exceed ZMW10,000.00; and

(e) a customer whose monthly average withdrawals do not exceed ZMW10,000.00.

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

(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 transaction equal to or less than ZMW10,000.00;

(b) a life insurance policy where the annual premium is not more than ZMW5,000.00 or a single premium of not more than 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 include—

(a) a country identified by sources such as mutual evaluation or detailed assessment reports, as having an effective anti-money laundering and countering terrorism or proliferation financing; 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 risk factors specified in this Part where the risk of money laundering or terrorism or proliferation financing may be high.

1. Customer risk factors include—

(a) the business relationship conducted in unusual circumstances such as significant unexplained geographic distance between the financial institution and the customer;

(b) a non-resident customer;

(c) a private banking customer;

(d) a legal person or legal arrangement that is a personal asset holding vehicle established for holding assets for investment purposes;

(e) a prominent influential person;

(f) a customer who originates from a high risk country;

(g) a customer that performs a transaction on behalf of another person, whether the identity of such other person is disclosed or not;

(h) a company that has nominee shareholders or shares in bearer form;

(i) a business that is cash-intensive; and

(j) 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 include—

(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, terrorism or proliferation financing;

(b) countries subject to sanctions, embargos or similar measures issued by the United Nations, Financial Action Task Force 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 include —

(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.

THIRD SCHEDULE
(Regulation 12)

MEASURES TO APPLY TO A CLASS OF NON-GOVERNMENTAL ORGANISATION

Part A (Measures by Competent Authority)

1. A competent authority shall identify a non-governmental organisation that is a legal person, arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal, or for the carrying out of other types of good works.

2. A competent authority shall use all relevant sources of information to identify the non-governmental organisations which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse from among those that fall within the description of non-governmental organisations referred to in paragraph 1.

3. An effective approach in identifying, preventing and combating terrorist financing abuse of non-governmental organisations shall involve the following elements:

(a) sustained outreach concerning terrorist financing issues;

(b) targeted risk-based supervision or monitoring;

(c) effective investigation and information gathering; and

(d) effective mechanisms for international cooperation.

4. A competent authority shall put in place measures to identify the nature of threats posed by terrorist entities to the non-governmental organisations which are at risk as well as how terrorist actors abuse those non-governmental organisations.

5. A competent authority shall periodically reassess the non-governmental organisation sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

6. A competent authority shall identify appropriate points of contact and procedures to respond to international requests for information regarding particular non-governmental organisations suspected of terrorist financing or involvement in other forms of terrorist support.

7. The Registrar for Non-Governmental Organisations or any other competent authority shall promptly inform the Centre where there is information that a non-governmental organisation is —

(a) involved in terrorist financing abuse or is a front for fundraising by a terrorist organisation;

(b) being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or

(c) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations.

8. A competent authority shall without delay freeze, in accordance with the procedure and process provided for under the Anti-Terrorism and Non-Proliferation Act, No. 6 of 2018, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity, including a nongovernmental organisation, that is either—

(a) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nation, and resolution 1267 (1999) and its successor resolutions; or

(b) designated by that country pursuant to resolution 1373.

9. A competent authority shall undertake targeted riskbased supervision or monitoring of a non-governmental organisation for purposes of enforcing compliance of measures for preventing or combating terrorist financing abuse of a non-governmental organisation.

Part B (Measures by Non-Governmental Organisations)

10. A non-governmental organisation shall put in place targeted measures provided in this Part which are in line with the riskbased approach to safeguard themselves from potential terrorist financing abuse.

11. A non-governmental organisation shall —

(a) maintain information on the purpose and objectives of their stated activities and the identity of the person who owns, controls or directs their activities, including senior officers, board members and trustees;

(b) issue annual financial statements providing breakdowns of incomes and expenditures;

(c) have in place appropriate controls to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of its stated activities;

(d) take reasonable measures to confirm the identity, credentials and good standing of beneficiaries and an associate non-governmental organisation and that they are not involved with or using the charitable funds to support terrorists or terrorist organisations; and

(e) maintain records of domestic and international transactions that are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the organisation.

12. A non-governmental organisation shall make available to a competent authority the information in paragraph 11*(a)* to *(e)* when required.

13. A non-governmental organisation shall carry out an assessment that estimates the risk of terrorism financing posed by its operations and business, its donors, its beneficiaries and any technology to its operation.

(1) Oganisational Risk Assessment

(a) The organisational risk assessment shall be—

(i) undertaken as soon as reasonably practicable after the non-governmental organisation commences operations;

(ii) recorded in order to demonstrate its basis; and

(iii) regularly reviewed and whenever necessary amended so as to keep the assessment uptodate.

(b) The organisational risk assessment shall have regard to all relevant risk factors, including

(i) the nature, scale and complexity of the nongovernmental organisation's activities;

(ii) any relevant findings of the most recent National Risk Assessment relating to the country;

(iii) the products and services provided by the non-governmental organisation;

(iv) the manner in which the products and services are provided, including whether the non-governmental organisation meets its beneficiaries; and

(v) any donor risk assessment, beneficiary risk assessment and technology risk assessment.

(2) Donor Risk Assessment

(a) A non-governmental organisation shall carry out an assessment that estimates the risk of terrorism financing posed by the non-governmental organisation's donor.

(b) A donor risk assessment shall be—

(i) undertaken prior to the establishment of a donor relationship with a donor;

(ii) recorded in order to demonstrate its basis; and

(iii) regularly reviewed, if appropriate, amended so as to keep the assessment uptodate and details of any review shall be recorded.

(c) The donor risk assessment shall have regard to all relevant risk factors, including—

(i) the organisational risk assessment carried out under paragraph 13 (1);

(ii) the location of the donor's activities;

(iii) the risk factors that pose a higher risk of terrorism financing in relation to a donor relationship;

(iv) the involvement of any third parties in the donor relationship; and

(v) whether the non-governmental organisation and the donor have met during the donor relationship or its formation.

(3) Beneficiary risk assessment

(a) A non-governmental organisation shall carry out an assessment that estimates the risk of terrorism financing posed by the non-governmental organisation's beneficiary.

(b) A beneficiary risk assessment shall be—

(i) undertaken prior to the establishment of a beneficiary relationship with a beneficiary;

(ii) recorded in order to be able to demonstrate its basis; and

(iii) regularly reviewed if appropriate, amended so as to keep the assessment uptodate and details of any review shall be recorded.

(c) The beneficiary risk assessment shall have regard to all relevant risk factors including—

(i) the organisational risk assessment carried out under paragraph 13 (1);

(ii) the nature, scale, complexity and location of the beneficiary's activities;

(iii) the persons to whom and the manner in which the products and services are provided;

(iv) the risk factors that pose a higher risk of terrorism financing in relation to a beneficiary;

(v) the involvement of any third parties within the beneficiary relationship and the process of remitting funds to the beneficiary; and

(vi) whether the non-governmental organisation and the beneficiary have met during the beneficiary relationship or its formation.

(4) Technology risk assessment

(a) A non-governmental organisation shall carry out an assessment that estimates the risk of money laundering and terrorism financing posed by any technology to the non-governmental organisation's business.

(b) The technology risk assessment shall be—

(i) undertaken as soon as reasonably practicable following the commencement of the measures specified in this Schedule or, where applicable, after the non-governmental organisation commences operations;

(ii) undertaken prior to the launch or implementation of new products, new business practices and delivery methods including new delivery systems;

(iii) undertaken prior to the use of new or developing technologies for both new and existing products and services;

(iv) recorded in order to be able to demonstrate its basis; and

(v) regularly reviewed and, if appropriate, amended so as to keep it up-to-date and details of any review shall be recorded.

(c) The technology risk assessment shall have regard to all relevant risk factors including—

(i) technology used by the non-governmental organisation to comply with Anti-Money Laundering/Combating Financing of Terrorism legislation;

(ii) the organisational risk assessment carried out under paragraph 13 (1);

(iii) the products and services provided by the non-governmental organisation;

(iv) the manner in which the products and services are provided by the non-governmental organisation, considering delivery methods, communication channels and payment mechanisms;

(v) digital information and document storage;

(vi) electronic verification of documents; and

(vii) data and transaction screening systems.

14. *(a)* A non-governmental organisation shall wherever feasible conduct transactions through regulated financial channels.

(b) A non-governmental organisation shall maintain information which may be publicly available either directly from the non-governmental organisation or through a relevant competent authority on the—

(i) purpose and objectives of their stated activities; and

(ii) identity of the person who owns, controls or directs activities of the non-governmental organisation, including senior officers, board members and trustees.

(c) A non-governmental organisation shall have appropriate controls in place to ensure that all funds are fully accounted for and spent in a manner that is consistent with the purpose and objectives of the non-governmental organisation's stated activities.

(d) A non-governmental organisation shall issue annual financial statements that provide detailed breakdowns of incomes and expenditures.

15. *(a)* A non-governmental organisation shall be required to take reasonable measures to document the identity of each donor.

(b) A non-governmental organisation shall, in relation to each donor relationship, establish, record, maintain and operate the following procedures and controls:

(i) obtain and maintain information on the identity of the donor; and

(ii) take reasonable measures to establish the source of funds or donations.

(c) A non-governmental organisations shall, where the source of funds or donation is assessed as posing a higher risk of terrorism financing, obtain additional information from the donor.

(d) The procedures and controls refered to under subparagraph *(b)* shall be undertaken either before a donor relationship is entered into or during the formation of that donor relationship.

(e) Where the requirements referred to underr subparagraph *(a)* are not met, the procedures and controls shall provide that—

(i) the donor relationship shall be terminated; and

(ii) the non-governmental organisation shall consider submitting a report to the Registrar for Non-Governmental Organisations or other relevant competent authority.

16. *(a)* A non-governmental organisation shall be required to take reasonable measures to confirm the identity, credentials and good standing of the beneficiary.

(b) A non-governmental organisation shall, in relation to a new beneficiary relationship, establish, record, maintain and operate the following procedures and controls:

(i) obtain and maintain information on the identity of the beneficiary;

(ii) confirm the identity of the beneficiary using reliable, independent source documents, data or information; and

(iii) obtain information on the nature and intended purpose of the beneficiary relationship.

(c) The procedures and controls referred to under subparagraph (b) shall be undertaken either before a new beneficiary relationship is entered into or during the formation of that beneficiary relationship.

(d) In exceptional circumstances, the confirmation of the identity of the beneficiary may be undertaken after the formation of the beneficiary relationship if—

(i) it occurs as soon as reasonably practicable;

(ii) the delay is essential so as not to interrupt the normal course of remitting funds to the beneficiary;

(iii) the beneficiary has not been identified as posing a higher risk of terrorism financing;

(iv) the risks of terrorism financing are effectively managed;

(v) the non-governmental organisation has not identified any unusual activity or suspicious activity;

(vi) the non-governmental organisations' senior management has approved the establishment of the beneficiary relationship and any subsequent activity; and

(vii) the non-governmental organisation ensures that the amount, type and number of transactions is appropriately limited and monitored.

(e) Except as provided in subparagraph (c), where the requirements of this paragraph are not met, the procedures and controls shallprovide that the—

(i) beneficiary relationship shall proceed no further;

(ii) non-governmental organisation shall terminate the beneficiary relationship; and

(iii) non-governmental organisation shall consider making a report to the Registrar of Non-Governmental Organistions.

17. *(a)* A non-governmental organisation shall be required to take reasonable measures to confirm the identity, credentials and good standing of each continuing donor, beneficiary or associate non-governmental organisation relationship.

(b) A non-governmental organisation shall, in relation to each continuing donor, beneficiary or associate non-governmental organisation relationship, record, maintain and operate the following procedures and controls:

(i) an examination of the background and purpose of the donor, beneficiary or associate non-governmental organisation relationship;

(ii) if satisfactory verification of the customer's identity was not obtained or produced, requiring such verification to be obtained or produced;

(iii) if satisfactory verification of the customer's identity was obtained or produced, a determination as to whether it is satisfactory; and

(iv) if confirmation of the beneficiary's identity is not satisfactory for any reason, reqruiring that the non-governmental organisation takes measures to confirm the beneficiary's identity.

(c) the procedures and controls shall be undertaken during a donor, beneficiary or associate non-governmental organisation relationship as soon as reasonably practicable.

(d) the non-governmental organisation shall keep written records of any examination, steps, measures or determination made or taken under this paragraph.

(e) except as provided with regard to exemptions and simplified measures, where the requirements of this paragraph are not met within a reasonable timeframe, the procedures and controls shall provide that the—

(i) donor, beneficiary or associate non-governmental organisation relationship shall proceed no further;

(ii) non-governmental organisation shall consider terminating the donor, beneficiary or associate non-governmental organisation; and

(iii) non-governmental organisation shall consider making a report to the Registrar of Non-Governmental Organisations.

18. **Record Keeping by a non-governmental organisation**

A non-governmental organisation shall keep for at least ten years

(a) a copy of the documents obtained or produced under risk based assessments:

(b) identification information on donors, beneficiaries and associate non-governmental organisations;

(c) account files;

(d) a record of all transactions carried out by the non-governmental organisation in fulfilling its objectives.; and

(e) such other records as are sufficient to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the non-governmental organisation.

19. A non-governmental organisation with information on a suspected case of terrorism financing may report it to a law enforcement agency, the Centre or any relevant competent authority.

FOURTH SCHEDULE
(Regulation 13)

Obligations Of An Accountable Institution

1. **Identification and Verification of Customer Identities**

1.1 An accountable institution shall conduct customer due diligence at the time of opening an account for, or otherwise establishing a business relationship with a customer by—

(a) identifying the customer; and

(b) verifying the identity of the customer using reliable, independent source documents, data or information.

1.2 An accountable institution shall verify the full name and physical address, and date and place of birth or a mobile number linked to a registered international mobile equipment identity number or sim card in place of physical address by comparing the particulars with

(a) the customer's driving licence, passport or national identification document bearing the individual's pictorial image; or

(b) 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.

1.3 An accountable institution shall verify the particulars of a body corporate by—

(a) 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;

(b) 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

(c) except for statutory bodies, the particulars of every person exercising direct or indirect control, for purposes of identifying the beneficial owner.

1.4 Where the customer is a legal arrangement, an accountable institution shall verify the particulars obtained in respect of the trust by comparing the name of the trustee, the settlor, beneficiary and any other natural person exercising ultimate effective control over the trust, with the trust deed or other founding document in terms of which the trust is created.

2. **Request for information**

The Director-General may request an accountable institution to provide information that the Centre may require for the performance of the Centre's functions under the Act and these Regulations.

3. **Currency transactions**

An accountable institution shall, not later than three working days after the transaction, report a currency transaction equal to or above the kwacha equivalent of USD10,000, whether denominated in Zambian kwacha or a foreign currency.

4. **Record Keeping**

An accountable institution shall maintain a record with respect to the accountable institution's customers and transactions for at least ten years from the date of transaction.

S. MUSOKOTWANE,
Minister of Finance and National Planning

LUSAKA
29th July, 2022
[MF/IDM/101/19/15]