




Financial Intelligence Centre

Republic of Zambia

**ANTI-MONEY LAUNDERING/ COUNTERING THE FINANCING OF TERRORISM AND
PROLIFERATION (AML/CFTP) GUIDELINES FOR VIRTUAL ASSET SERVICE PROVIDERS
(VASPs)**

This document is authorized by:

Name	Title	Date	Signature
Mrs. Liya Tembo	Acting Director General	29.12.2022	

Version Control:

Version	Date	Status	Author
1.0	29.12.2022	First review	Compliance & Prevention Department

TABLE OF CONTENTS

1.0	INTRODUCTION	3
2.0	DEFINITION OF KEY TERMS	4
3.0	OVERVIEW OF VIRTUAL ASSET SERVICE PROVIDERS	6
4.0	SCOPE OF GUIDELINES	8
5.0	COMPLIANCE OBLIGATIONS	8
5.1	COMPLIANCE PROGRAM	8
5.1.1	AML/CFTP Policy, Procedures and Internal Controls	8
5.1.2	Compliance Officer	9
5.1.3	Training	10
5.1.4	Audit	11
5.2	SUSPICIOUS TRANSACTION REPORTING	11
5.2.1	Obligation to Report Suspicious Transactions	11
5.2.2	Prohibition against Tipping Off	12
5.2.3	Protection of identity of persons and information relating to STRs	12
5.2.4	Exemption from liability for good faith reporting of suspicious transactions	12
5.3	SANCTION SCREENING	13
5.4	RECORD KEEPING	13
5.5	MONITORING OF COMPLIANCE PROGRAM	14
6.0	CUSTOMER DUE DILIGENCE	14
6.1	CUSTOMER DUE DILIGENCE PROCEDURES	14
6.2	HIGH-RISK CATEGORIES OF CUSTOMERS	16
7.0	WIRE TRANSFERS	17
8.0	REGISTRATION	18
9.0	FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS	18

1.0 INTRODUCTION

Financial technology presents enormous opportunities as well as potentially significant risks to the integrity of the financial system. This is particularly the case with virtual assets (VAs). Virtual assets such as cryptocurrency have the potential to improve payment efficiency, reduce transaction costs and improve financial inclusion because they enable greater speed, lower costs, and increased efficiency in making payments and transfers. However, literature and typologies published point to the potential for misuse of virtual assets by criminals and those who would want to fund illicit activities.

Virtual Asset Service Providers (VASPs) are designated as 'reporting entities' under the Financial Intelligence Centre (FIC) Act No. 46 of 2010 (as amended) (the Act). According to Section 2 of the FIC Act No. 16 of 2020 a reporting entity means an institution required to make a report under the Act, which is regulated by a Supervisory Authority and includes a financial service provider, a designated non-financial business or profession or a virtual asset service provider (VASP). VASPs may offer a diverse range of services, including transferring money or value for, or on behalf of, a customer', 'money or currency changing', or 'investing, administering, or managing funds or money on behalf of other persons'.

The Financial Intelligence Centre (the FIC or Centre) is an independent and autonomous body corporate established under the Financial Intelligence Centre Act No. 46 of 2010 (as amended). The Centre's core mandate is to receive and analyse Suspicious Transaction Reports (STRs), any other information relevant to money laundering (ML), terrorism financing (TF) and proliferation financing (PF) and serious offences relating to ML, TF or PF for dissemination of financial intelligence reports to relevant competent authorities for investigation and prosecution where there are reasonable grounds to suspect that crimes have been committed.

Section 56 of the FIC Act) empowers the FIC to issue guidelines to reporting entities to ensure that they are compliant with the provisions of the Act. These guidelines have been issued to provide guidance to VASPs on their legal obligations and measures to prevent and detect money laundering, financing of terrorism and proliferation activities and to assist industry players to comply with the Act.

2.0 DEFINITION OF KEY TERMS

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

Financial Action Task Force (FATF): Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

Money Laundering offence: A money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of crime (e.g. money) knowing or believing that these were derived from the commission of a designated offence. Examples of designated offences include, drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation and tax crimes.

Proliferation financing: Section 2 of the Anti-Terrorism and Non Proliferation Act defines Proliferation Financing as an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services to be used or knowing that they are to be used in whole or in part for proliferation, the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, supply, sale or use of nuclear, ballistic, chemical, radiological or biological weapons or any other weapon capable of causing mass destruction and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, including technology, goods, software, services or expertise, in contravention of the Anti-Terrorism and Non-Proliferation Act or, where applicable, international obligations derived from relevant United Nations Security Council Resolutions.

Prominent Influential Persons (PIPs): An individual who is or has been entrusted with a prominent public function by a State or an international or local body or organization but is not of middle or junior ranking. Section

2 of the FIC Act No. 16 of 2020 provides detailed definition of a Prominent Influential Person.

Reporting Entity: Reporting Entity means an institution required to make reports under the FIC Act which is regulated by a Supervisory Authority, and includes a financial service provider, a designated non-financial business or profession or a Virtual Asset Service Provider. The reports that are filed to the FIC include Suspicious Transaction and Currency Transaction Reports.

Suspicious Transaction Report: Section 2 of the FIC Act defines a Suspicious Transaction Report as a report submitted on suspected or attempted money laundering, financing of terrorism or proliferation or any other serious offence whether in form of a data message or otherwise.

Terrorism Financing: Section 2 of the Anti-Terrorism and Non-Proliferation Act defines terrorism financing as an act by any person who, irrespective of whether a terrorist act occurs, by any means, directly or indirectly, willfully provides or collects funds or attempts to do so with the intention that the funds should be used or knowing that the funds are to be used in full or in part— (i) to carry out a terrorist act; (ii) by a terrorist; (iii) by a terrorist organisation; or (iv) for the travel of a person to a State other than the person's State of residence or nationality for the purpose of perpetration, planning or preparation of, or participation in, terrorist act or the providing or receiving of terrorist training.

Virtual Asset¹: Section 2 of the FIC Act defines a virtual asset as a convertible virtual asset such as crypto currency or other digital means of exchange where the virtual asset is accepted by a person as a means of payment for goods or services, a unit of account, a store of value or a commodity.

Virtual Asset Service Provider: Section 2 of the FIC Act defines a virtual asset service provider as any person who as a business, conducts one or more of the following activities or operations for or on behalf of another person:

- i. exchange between virtual assets and fiat currencies;
- ii. exchange between one or more forms of virtual assets;

¹ Virtual Assets do not include digital representation of fiat currencies, securities and other financial assets.

- iii. transfer of virtual assets;
- iv. safekeeping and/or administration of virtual asset instruments enabling control over virtual assets;
- v. participation in and provision of financial services related to an issuer's offer and sale of a virtual asset;
- vi. provision of intermediary services for the buying and selling of virtual assets, including through the use of virtual asset vending machine facilities.

Wire Transfer: Section 2 of the FIC Act defines a wire transfer as any transaction carried out on behalf of an originator, through a financial service provider or payment system including an institution that originates the wire transfer and an intermediary institution that participates in completion of the transfer, by electronic means, with a view to making an amount of money available to a beneficiary.

3.0 OVERVIEW OF VIRTUAL ASSET SERVICE PROVIDERS

As of September 2022, Africa had the second largest number of crypto users in the world after Asia. In Zambia, trading in virtual assets is a growing trend which has emerged in the context of limited regulation. However, within the global AML/CFTF space, the Financial Action Task Force (FATF) has updated the standards to include the regulation of Virtual Assets and Virtual Asset Service Providers for AML/CFTF purposes. The FATF Recommendation 15 outlines requirements that VASPs have to adhere to in their operations. Further, the FATF recommendations (June 2019) require countries to ensure that VASPs are licensed or registered and subjected to effective systems for monitoring or supervision by a competent authority.

Like other new payment methods, virtual assets have legitimate use and come with both benefits and risks. Virtual Assets hold the promise of making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank. It should, however, be noted that the threat of misuse of virtual assets to commit fraud, theft, ML and TF is serious.

Some key ML/TF vulnerabilities and high risk factors that are associated with VASPs include:

- i. The initial purchase of a virtual asset will usually involve the exchange of fiat currency to virtual asset. The conversion to and from fiat currency is the point where a launderer is most exposed – this is particularly relevant for a VASP that operates as an exchange;
- ii. VASPs often utilise *non-face-to-face business relationships*. This is a risk factor for ML/TF as customers may hide their true identity to avoid sanctions or attention from law enforcement;
- iii. VASPs should be aware of risks involving customers who conduct transactions with wallets or virtual assets that have been *linked to darknet marketplaces* or other illicit activity;
- iv. The use of virtual assets to avoid international sanctions is a known risk. As regimes and individuals are cut off from the global financial system, they search for alternatives. This has resulted in some countries and individuals trying to turn to digital currencies to offset the impact of economic sanctions;
- v. Virtual Assets have a global reach, which increases the risks of potential ML/TF. Virtual asset systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and transfer funds with customers avoiding face-to-face interaction, thus enhancing anonymity;
- vi. The risk of TF is significant – terrorist organisations and their supporters and sympathisers are constantly looking for ways to raise and transfer funds without detection or tracking by law enforcement, and the level of anonymity that virtual assets can provide is attractive to them;
- vii. The size of VASPs can vary, but the technology in most cases will allow for *rapid expansion*. This could lead to VASPs becoming overwhelmed and unable to complete thorough customer due diligence (CDD) or transaction monitoring.

4.0 SCOPE OF GUIDELINES

The VASP guidelines have incorporated relevant provisions in the FIC Act, FATF-Recommendations and FATF Guidelines and other international best practices in the AML/CFTP regime. These Guidelines cover among others the following key areas of AML/CFTP policy; customer due diligence, the AML/CFTP Compliance programme, record keeping, sanction screening and reporting of suspicious transactions.

These Guidelines are provided as general information only and as such do not represent all the requirements under the law. The Guidelines do not constitute legal advice and are not intended to replace the FIC Act or any other guidelines, directives or regulations issued by the Centre.

5.0 COMPLIANCE OBLIGATIONS

5.1 COMPLIANCE PROGRAM

An AML/CFTP Compliance program is an important component of an institution's AML/CFTP compliance regime. The primary goal of the compliance program is to protect the institution against ML/TF/PF and to ensure that the institution is in full compliance with relevant AML/CFTP laws. The AML/CFTP compliance program has four (4) components, namely the development of internal controls, policies and procedures; appointment of a compliance officer; training of staff; and conducting an independent audit of the compliance program.

5.1.1 AML/CFTP Policy, Procedures and Internal Controls

VASPs shall adopt policies indicating their commitment to comply with AML/CFTP obligations under the relevant Acts and regulations to prevent any transaction that facilitates ML/TF/PF activities. The VASP shall formulate and implement internal rules procedures and other controls that will deter criminals from using its services for ML/TF/PF and ensure that its obligations under the relevant laws are always met. These procedures, policies and controls should cover the customer due diligence (CDD), record keeping, the detection and reporting of unusual and suspicious transactions, sanction

screening, transaction monitoring and risk assessment, among other things.

5.1.2 Compliance Officer

A VASP should designate a Compliance Officer who is at senior management level within its organisation who shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. Appointing a compliance officer is the first step towards compliance. The designated Compliance Officer should have 2 years' experience in regulatory compliance, should not have been convicted of an offence under the FIC Act or any other law and should be certified and approved by the FIC.

The Compliance Officer shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFTP compliance programme. The Compliance Officer shall have ready access to all the books, records and employees of the VASP necessary to fulfil the responsibilities under the FIC Act. If the VASP is a sole operator, they are expected to act as the compliance officer themselves and take full responsibility for all compliance requirements.

An employee of a VASP shall promptly report to a designated Compliance Officer all cases where: a) the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that a customer has been or is involved in an illegal activity or crime; or b) a customer in respect of whom the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that another customer has been engaging in illegal activities or crimes.

The duties of the Compliance Officer shall include but shall not be limited to the following:

- i. Developing an AML/CFTP Compliance Program;

- ii. Receiving and vetting suspicious transaction reports from staff;
- iii. Submitting suspicious transaction reports to the Centre;
- iv. Ensuring that the reporting entity's compliance program is implemented;
- v. Co-ordinating the training of staff in AML/CFTP awareness, detection methods and reporting requirements; and
- vi. Serving both as a liaison officer with the Centre as well as a point-of-contact for all employees on issues relating to ML/TF/PF. The reporting entity shall ensure that the Compliance Officer has access to other information that may be of assistance to him/her in consideration of a suspicious or unusual transaction.

In designating a Compliance officer, the VASP shall submit the following to the FIC:

- a) A letter addressed to the Director General of the FIC appointing the officer;
- b) A completed Compliance Officer Vetting Form;
- c) A copy of the National Registration Card (NRC) or passport of the appointed Compliance Officer;
- d) The latest Curriculum Vitae (CV) of the appointed Compliance Officer.

Once approved by the FIC, the VASP should ensure that the designated compliance officer is provided with credentials to the online reporting portal.

5.1.3 Training

The FIC Act requires reporting entities to have formal, written AML/CFTP Compliance programs that include training. Ongoing employee training programs should be in place in all VASPs to ensure that employees are kept informed of new developments, including information on current ML / TF/ PF techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFTP laws and obligations, and in particular, requirements concerning CDD and

suspicious transaction reporting. The timing, coverage and content of the employee training program should be tailored to meet the perceived needs of the reporting entity. VASPs should ensure that the board of directors, management and staff are included in the training program. Where there is limited knowledge, the VASP may request competent authorities such as the FIC to conduct the training.

5.1.4 Audit

Reporting entities including VASPs are required to have an independent audit performed by officers not involved with the entity's AML/CFTP Compliance function to test compliance with the procedures, policies and controls. The individuals conducting the audit should report directly to the board of directors or to a designated board committee. The VASP should document the findings and recommendations of the audit on AML/CFTP matters and the board of directors should ensure that any identified deficiencies are addressed.

5.2 SUSPICIOUS TRANSACTION REPORTING

5.2.1 Obligation to Report Suspicious Transactions

Whenever a VASP processes a transaction to which there are reasonable grounds to suspect that a property is the proceeds of crime, or is related to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or persons who finance terrorism, it should take reasonable measures to ascertain the purpose of that transaction and submit a report to the Centre, setting out the suspicion, within three (3) working days of forming that suspicion. The STR should be submitted through the online reporting portal. The designated Compliance Officer is responsible for the submission of STRs to the Centre using the online reporting portal.

Further, a VASP is required to exercise caution when carrying out a transaction which it suspects to be related to ML/TF/PF. This may involve delaying the completion of transaction while undertaking background checks on the customer. Where it is

established that the transaction is linked to suspected ML/TF/PF this should trigger filing of an STR to the FIC. The Act also requires an STR to be submitted on attempted ML/TF/PF.

Failure to submit a STR to the Centre may lead to imprisonment upon conviction to a term of up to seven (7) years or payment of a fine of seven hundred thousand penalty units or to both.

5.2.2 Prohibition against Tipping Off

A VASP or any director, partner, officer, principal or employee of the VASP is not allowed to disclose to any person the contents of the STR Form. Further, the disclosure of any other information from which a person could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made is prohibited. Any person who contravenes this requirement commits an offence and is liable to a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five (5) years, or to both.

5.2.3 Protection of identity of persons and information relating to STRs

A VASP is not allowed to disclose any information that identifies, or is likely to identify the person who prepared or made a suspicious transaction report, or handled the underlying transaction. Such disclosure is an offence which may result in a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five (5) years, or to both.

5.2.4 Exemption from liability for good faith reporting of suspicious transactions

No civil, criminal, administrative or disciplinary proceedings for breach of banking or professional secrecy or contract shall be taken against an individual for submitting a completed

STR form, in good faith, or in compliance with directions given by the FIC Act.

5.3 SANCTION SCREENING

Sanctions screening is a control used in the detection, prevention and disruption of financial crimes. It is designed to identify targeted individuals or entities during on-boarding or the lifecycle of the customer relationship.

The Anti-Terrorism and Non-Proliferation Act No. 6 of 2018 and other domestic regulations prohibit reporting entities from entering in a business relationship or engaging in any transaction with a sanctioned person or entity on the United Nations Security Council (UNSC) sanctions list. This entails that VASPs should on a regular basis screen their customers (potential and existing) to ensure that they are not on the sanctions list. In relation to implementation of Targeted Financial Sanctions concerning TF or PF, VASP should freeze the assets of the customer where there is a positive match, during screening of customers against the sanctions list and should without delay report to the National Anti-Terrorism Centre and supervisory authorities including the FIC.

5.4 RECORD KEEPING

VASPs are required to keep adequate records as outlined in Section 22 of the FIC Act (as amended).

A VASP shall maintain all books and records relating to its customers and transactions for a period of at least ten (10) years after the business relationship has ended or from the date of the transaction. The VASP shall further ensure that those records and underlying information are available on a timely basis to the FIC or other competent authorities.

5.5 MONITORING OF COMPLIANCE PROGRAM

The FIC will from time to time undertake monitoring activities and on-site inspections to VASPs to monitor how the AML/CFTP Compliance programs are being implemented.

6.0 CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) is the identification and verification of both the customer and beneficiary including but not limited to continuous monitoring of the business relationship with the reporting entity.

Part III of the Act requires reporting entities to institute measures to ensure effective CDD at all times. VASPs shall undertake measures when:

- i. Establishing a business relationship with or conducting a business transaction for a customer;
- ii. Carrying out a transaction in an amount equal to or above US\$1000 including where the transaction is carried out in a single operation or several operations that appear to be linked;
- iii. The Customer wishes to carry out a domestic or international wire transfer of monetary amounts in the amounts equal to, or above, US\$ 1000
- iv. There is a suspicion of money laundering or terrorist financing;
- v. There are doubts about the veracity or adequacy of previously obtained customer identification data.

6.1 CUSTOMER DUE DILIGENCE PROCEDURES

- a) VASPs shall identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, such as a validly issued National Registration Card, Passport, Drivers' Licence, (which should not have expired at the time of conducting CDD), Certified Certificate of Incorporation or such other information as the Minister may prescribe;

- b) In respect of customers that are legal persons or legal arrangements, VASPs shall:

- i. verify any person purporting to have been authorised to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and
 - ii. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from a recognised established body or similar evidence of establishment or existence and any other relevant information.

- c) A VASP shall, where applicable, identify a beneficial-owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial-owner is;

- d) VASPS shall in respect of all customers determine whether or not a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the reporting entity shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person;

- e) VASPs shall take reasonable measures in respect of customers that are legal persons or legal arrangements to:
 - i. Understand the ownership and control structure of such a customer; and
 - ii. Determine the natural persons that ultimately own or control the customer. For trusts – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.

- f) A VASP shall obtain information on the purpose and intended nature of the business relationship of their potential customers;

- g) A VASP shall conduct ongoing due diligence on the business relationship with the customers. The ongoing due diligence includes scrutinizing the transactions undertaken by the customer throughout the course of the relationship to ensure that the transactions being conducted are consistent with the

reporting entity's knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).

- h) VASPs shall ensure that documents, data or information collected under the CDD-process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of higher-risk business relationships or customer categories. All books and records with respect to its customers and transactions should be maintained for a period of at least 10 years;

6.2 HIGH-RISK CATEGORIES OF CUSTOMERS

VASPs should have appropriate risk management systems to identify customers whose activities may pose a high risk of money laundering and terrorism financing. To this effect, they are required to exercise enhanced identification, verification and ongoing due diligence procedures with respect to High Risk Customers. VASPs shall perform enhanced due diligence for high-risk categories of customers, business relationships or transactions.

VASPs shall, in addition to performing CDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a Prominent Influential Person (PIP).

The risk management systems used by VASPs to identify customers whose activities may pose a high risk of money laundering and financing of terrorism shall require:-

- I. Enhanced identification-which involves identifying customers or activities engaged in by customers who may pose high risk of money laundering or financing of terrorism by taking into account:
 - a. the nature and business of customers;
 - b. customer activities, transaction patterns and operations;
 - c. geographic location of the customer and/or transaction
 - d. the magnitude of customer's assets that a reporting entity handles;
 - e. third parties that may be involved in the customer's activities;

- f. where applicable, the beneficial ownership of an entity and their impact on risk;
- g. any other indicators that may be relevant.

II. Verification and on-going Due Diligence-which includes:

- a) Seeking additional information beyond the minimum requirements under the law to substantiate the customer's identity or the beneficial ownership of an entity and
- b) Obtaining additional information about the intended nature and value of a given transaction.

VASPs shall obtain senior management approval before they establish a business relationship with a PIP. Where a customer has been accepted or has an ongoing relationship with the VASP and the customer or beneficial-owner is subsequently found to be or becomes a PIP, a VASP is required to obtain senior management approval in order to continue the business relationship. VASPs shall take reasonable measures to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PIPs and report all anomalies or unusual and abnormal transactions immediately to the FIC.

7.0 WIRE TRANSFERS

Wire transfers are an important activity for VASPs. Preventing and detecting ML/TF/PF requires VASPs to know who the originator and beneficiary of the transaction are and where applicable, intermediary institutions. As a result, some information, such as the identity of both parties, must “travel” with the Virtual Asset (VA), similar to how it accompanies a wire transfer between banks—this is commonly called the “*travel rule*”. When transferring VAs, VASPs must therefore obtain, hold, and transmit required originator and beneficiary information.

With respect to wire transfers, the requirements set out in Regulation 6 (1),(6-30) of SI No. 53 of 2022 The Financial Intelligence Centre (Prescribed Threshold) Regulations, 2022 apply to virtual asset service providers.

VASPs shall adopt risk based policies and procedures for dealing with the transfer of virtual assets.

8.0 REGISTRATION

Pursuant to Regulation 20(2) and (3) of the FIC (General) Regulations, SI No. 54 of 2022 requires a VASP to be registered or licensed in the jurisdiction where the VASP is created or place of business is located by a designated supervisory authority for the purpose of the Centre supervising and enforcing compliance under the FIC Act. Under Section 5 of the FIC Act, the FIC is empowered to supervise sectors for AML/CFTP where no specific supervisor is designated. In this regard, the FIC is the AML/CFTP supervisor for the VASPs. Therefore, in addition to the requisite registration from the Patents and Companies Registration Agency (PACRA), VASPS are required to register with the Centre.

The following information should be provided to the FIC to complete the VASP registration process:

1. Company Profile
2. Certificate of Incorporation
3. Latest PACRA Printout
4. Tax Clearance Certificate
5. Beneficial Ownership information (name, physical address, ID number, occupation & gender)
6. Google Map Coordinates of your place of operation (physical address)

9.0 FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS

For any inquiries relating to these guidelines please contact the FIC using the address below:

The Director General
Financial Intelligence Centre
P O Box 30481
Lusaka
ZAMBIA

ISSUED BY THE FINANCIAL INTELLIGENCE CENTRE
DECEMBER, 2022
