



REPUBLIC OF ZAMBIA

GOVERNMENT GAZETTE

Published by Authority

Price: K35.00 net
Annual Subscription: K900.00

No. 7991]

Lusaka, Friday, 18th September, 2026

[Vol. LXII, No. 130

GAZETTE NOTICE No. 1439 of 2026

[11289792

The National Payment Systems Act

(Act No. 1 of 2007)

The Bank of Zambia Directives on Virtual Assets, 2026

WHEREAS the Bank is responsible for regulating, overseeing and maintaining an efficient and safe payment system in Zambia; and

WHEREAS it is the intention of the Bank to protect the integrity of the payment, clearing and settlement system.

NOW THEREFORE, in exercise of the powers contained in section forty-three of the National Payment Systems Act, 2007 the following Directives are hereby made.

PART I

PRELIMINARY

Short title

1. These Directives may be cited as the Bank of Zambia Directives on Virtual Assets, 2026.

Application

2. (1) These Directives shall apply to any person providing virtual asset services in or from Zambia.
- (2) These Directives shall not apply to—
 - (a) transactions in which a person grants a value as part of an affinity or rewards program, which value cannot be taken from or exchanged with the person for legal tender, bank credit or any virtual asset;
 - (b) a digital representation of value issued by or on behalf of the publisher and used within an online game, game platform or game sold by the same publisher or offered on the same game platform;
 - (c) non-fungible tokens or any virtual assets backed by non-fungible tokens; or
 - (d) electronic representations of fiat currency, security, or any other financial asset under the Bank of Zambia Act, the Banking and Financial Services Act, the National Payment Systems Act or any other relevant legislation.

Interpretation

3. In these Directives, unless the context otherwise requires:—

“Act” means the National Payment Systems Act, 2007;

“agent” means a person or entity engaged by a virtual asset service provider to provide marketing services on its behalf;

“asset” means any movable or immovable property of any nature, whether tangible or intangible, that holds economic or financial value and is owned or controlled by an individual or entity with legally enforceable rights or claims;

“bank” has the meaning assigned to the term in the Banking and Financial Services Act, 2017;

“Bank” has the meaning assigned to the term in the Bank of Zambia Act, 2022;

“beneficial owner” means a natural person who ultimately owns or controls a customer, or the person on whose behalf a transaction is being conducted and includes those natural persons who exercise ultimate effective control over a legal person or arrangement;

“board” means the governing body of a virtual asset service provider;

“comparable body” a body outside Zambia which has functions similar to those of the Bank with respect to the regulation and licensing of a virtual asset service provider;

“Competent Authority” has the meaning assigned to the term in the Financial Intelligence Centre Act, 2010;

“customer” has the meaning assigned to the term in the Financial Intelligence Centre Act, 2010;

“customer due diligence” means a process where a virtual asset service provider verifies the identity of their customers, including the beneficial owners, assesses the risks associated with their customers, and understand the purpose and nature of the business relationship;

“cyber security” has the meaning assigned to the term in the Cybersecurity Act, 2025;

“electronic money or e-money” has the meaning assigned to the term in the National Payment Systems Directives on Electronic Money Issuance, 2023;

“fiat currency” means—

(a) notes, coins or tokens issued into circulation by the Bank in terms of the Bank of Zambia Act; or

(b) notes, coins or money of a jurisdiction that is designated by the Government of that jurisdiction as legal tender;

“financial year” means in respect of—

(a) the virtual asset service provider’s first financial year, a period not exceeding 18 months from the date of incorporation or issue of a licence; and

(b) every subsequent financial year, a period not exceeding 12 months;

“holding account” has the meaning assigned to the term in the National Payment Systems Directives on Electronic Money Issuance, 2023;

“licence” means authorisation granted to conduct virtual assets business;

“non-fungible token” means a unique virtual token created for use in specific applications which cannot be—

(a) divided and is not interchangeable with any other type of virtual token; and

(b) sold in a secondary market;

“person” has the meaning assigned to the term in the Constitution;

“property” means asset of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, real or personal, and legal documents or instruments evidencing title to, or interest in such assets;

“senior officer” means a person responsible for—

(a) the day-to-day administration of the virtual asset service provider;

(b) finance;

(c) compliance;

(d) operations;

(e) information technology; or

(f) any other function as may be determined by the Bank;

“significant shareholder” has the meaning assigned to the term in the Banking and Financial Services Act;

"stablecoin" means a type of virtual currency whose value is pegged to a stable fiat currency held with a regulated financial service provider;

"suspicious transaction report" has the meaning assigned to it under the Financial Intelligence Centre Act, 2010;

"unsafe and unsound practice" means—

(a) conducting the affairs of a virtual asset service provider in a manner that is—

(i) detrimental to the stability of the financial sector or the interests of customers and creditors;

(ii) prejudicial to the interest of the virtual asset service provider; or

(iii) in contravention of these Directive or any other relevant written law;

(b) maintaining inadequate liquidity; or

(c) any other practice that the Bank may designate as unsafe and unsound practice;

"virtual asset" means a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the Financial Action Task Force Recommendations;

"virtual asset exchange" means a marketplace on a digital platform for the sale, purchase, transfer or exchange of a virtual asset for fiat currency or vice versa;

"virtual asset service provider" means any natural or legal person who, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

(a) exchange between virtual assets and fiat currencies;

(b) exchange between one or more forms of virtual assets;

(c) transfer of virtual assets;

(d) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

(e) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset;

"virtual currency" means a digital representation of value that can be digitally traded and function as a medium of exchange, a unit of account, or a store of value.

PART II

LICENSING OF VIRTUAL ASSET SERVICE PROVIDERS

Prohibition of unlicensed virtual asset service provider

4. (1) A person shall not operate as a virtual asset service provider without a licence.
- (2) A person who contravenes sub-directive (1) commits an offence and is liable upon conviction to a fine not exceeding two thousand five hundred penalty units, or imprisonment for a term not exceeding two years, or to both.

Application for licence

5. (1) A person intending to offer virtual asset services to the public shall apply to the Bank for a licence, except where such services involve securities or investment instruments, in which case regulatory oversight rests with the Securities and Exchange Commission in accordance with the Securities Act No. 41 of 2016.

(2) An application in sub directive (1) shall—

(a) be in such form and manner as may be determined by the Bank;

(b) have attached to it or contain the following —

(i) proof of the applicant's registration with a comparable body, where applicable;

(ii) Articles of Association and certified copies of proof of registration or certificate of incorporation of the entity;

(iii) permanent residential addresses of the applicant's directors and senior officers;

- (iv) business plan, including financial and operational projections covering at least three years, setting out the nature and scale of the virtual asset activities proposed to be carried out, and technological and staffing requirements;
- (v) detailed description of the product proposal, including end-to-end process flows and architecture;
- (vi) particulars of the applicant's arrangements for the management of the business and draft agreement(s) with partners, if any;
- (vii) policies and measures to be adopted by the applicant to meet the obligations under these Directives and the Financial Intelligence Centre Act;
- (viii) consumer protection arrangements, including customer complaint handling mechanism, data privacy and data security;
- (ix) certified copies of identification of the applicant's shareholders, ultimate beneficial owner(s), if any, directors and senior officers;
- (x) audited financial statements for the previous three years where the applicant is an established business;
- (xi) the source and evidence of availability of the applicant's capital;
- (xii) letter from an external audit firm confirming its appointment as the company's auditors;
- (xiii) a risk management framework to address inherent risks including operational risk, cyber security risk, liquidity risk, credit risk, data privacy risk and consumer protection risks;
- (xiv) for stablecoin business, arrangements around the account held with a financial service provider earmarked for holding fiat currency to be pegged to stablecoins, and mechanisms of how the stablecoin will be pegged to the fiat currency;
- (xv) internal controls and governance arrangements around the wallet to host virtual assets in trust for customers;
- (xvi) the applicant has sufficient underwritten insurance and/or other arrangements commensurate to the level of operational risk, including fraud;
- (xvii) General Tax Clearance Certificate (TCC);
- (xviii) proof of payment of an applicable licence fee as determined by the Bank;
- (xix) other additional information or documents as may be required by the Bank;

(3) A financial or payment service provider may, with the approval of the Bank, provide virtual asset services using a separately incorporated legal entity.

(4) An applicant may withdraw an application by giving seven days' written notice to the Bank at any time before the determination of the application.

Determination of the application

6. (1) The Bank shall determine the application for a licence within a period of ninety calendar days from the date of receipt of a duly completed application.

Grant of licence

7. (1) The Bank may, on application made under directive 5, grant a licence where it is satisfied with the submissions made and the applicant, its beneficial owners, their associates, and officers are fit and proper persons to provide virtual asset services for which the licence is sought.

(2) The Bank shall when determining whether a person is fit and proper under sub-directive (1), have regard to the Bank of Zambia Guidelines for the fit and proper assessment.

(3) The Bank may, in addition to sub-directive (2), take into account—

- (a) the virtual asset services proposed to be carried out by the applicant;
- (b) the capacity of the applicant to carry out the business activities;
- (c) any international standard relating to the provision of virtual asset services;

(d) any information obtained from a competent authority or comparable body; and

(e) whether the granting of a licence to the applicant may pose a risk to the public.

(4) The Bank may grant an applicant a licence in such form and manner as may be determined.

(5) A licence granted shall remain valid unless it is revoked by the Bank or surrendered by the virtual asset service provider.

Refusal to grant a licence

8. (1) The Bank may refuse to grant a licence where:

(a) the applicant does not meet the requirements listed under directive 5.

(b) the Bank determines that the product and services or the applicant may introduce systemic and other risks into the financial system.

Pre-launch inspection

9. (1) A virtual asset service provider shall not provide virtual asset services until the Bank conducts a pre-launch inspection.

(2) The pre-launch inspection shall be conducted in a manner and form as the Bank may deem necessary.

(3) The Bank shall not later than 14 business days after the pre-launch inspection inform the virtual asset service provider in writing on whether the premises and systems are suitable for commencement of business operations.

Display of Licence

10. (1) A virtual asset service provider shall display its licence in a prominent place at its administrative office and on its official website and/or other electronic sites.

(2) If a virtual asset service provider operates branches, it shall also display a certified copy of its licence in a prominent location at each branch where business is conducted

Licence not transferrable

11. A licence shall not be transferred, assigned or encumbered in any way.

Ongoing monitoring

12. (1) The Bank shall conduct ongoing monitoring and supervision of a virtual asset service provider using a risk based approach.

(2) Notwithstanding the generality of sub-directive (1), a virtual asset service provider shall submit monthly returns on:

(a) the volumes and values of transactions processed;

(b) Management accounts;

(c) List of virtual asset holders showing balances as at the reporting date;

(d) breakdown of the funds held in the virtual asset service provider's ecosystem according to the customers register;

(e) reconciliation of stablecoins held in the virtual asset service provider's ecosystem to the customers register;

(f) reconciliation between the customer funds held in a financial service provider and the electronic value in the virtual asset service provider's ecosystem;

(g) cybersecurity incidents experienced;

(h) security audit reports issued by auditors in the preceding period;

(i) Statistics on the suspicious transaction reports submitted to the Financial Intelligence Centre;

(j) system availability;

(k) customer complaints received and resolution thereof;

- (l) incidents of data privacy breaches and resolution thereof;
- (m) changes in the shareholding and ultimate shareholding, board and senior management structures;
- (n) changes in the information previously submitted to the Bank;
- (o) proof of appropriate insurance coverage or other measure taken to safeguard against potential losses; and
- (p) Any other returns that the Bank may deem necessary.

(3) The Bank may require a virtual asset service provider or any other entity it reasonably suspects of being involved in a virtual asset or stablecoin-related business to furnish it with details of any of its operations, or any other information as the Bank may deem necessary.

- (4) The Bank shall use a risk-based approach to the regulation and supervision of virtual asset service providers.

Cessation of virtual assets business

13. (1) A solvent virtual asset service provider may make a request to cease activities or operations as a virtual asset service provider.

(2) A virtual asset service provider under sub-directive (1) shall, within seven days of submitting the request, submit a written plan to the Bank setting out the steps the virtual asset service provider shall follow to ensure orderly exit from the market.

- (3) The plan in sub-directive (2) shall state—

- (a) the full names and physical address of the person who will manage the virtual asset service provider's cessation of the business;
- (b) the period required to cease the business operations;
- (c) the manner in which customer files or accounts will be closed and secured;
- (d) customer notification procedures;
- (e) customer transfer procedures, if applicable.

- (4) The Bank shall, upon receipt of the plan under sub-directive (2), supervise and monitor the execution of the plan.

- (5) In determining the request to cease activities or operations as a virtual asset Payment Systems Act and any other relevant laws.

(6) The Bank may, in the public interest and for purposes of this directive, give directions to the virtual asset service provider to cease provision of virtual asset services and the virtual asset service provider shall comply with such directions.

Suspension or revocation of licence

14. The Bank may suspend or revoke a licence where —

- (a) the Bank considers that the virtual asset service provider is not a fit and proper person in terms of these Directives;
- (b) the Bank considers that the virtual asset service provider does not fulfil the requirements of, or has contravened, any of the provisions of these Directives, or has failed to satisfy or comply with any obligation or condition to which the licence is subject;
- (c) the Bank is furnished, by or on behalf of the virtual asset service provider, with information which is false, inaccurate or misleading;
- (d) the virtual asset service provider has not commenced provision of services that it is authorised to provide within 12 months, from the date of granting of the licence, or has ceased to provide the virtual asset service;
- (e) the Bank considers it necessary to suspend or revoke the licence for the protection of customers and the public;
- (f) a virtual asset service provider makes a request for the suspension or revocation of the licence;
- (g) the virtual asset service provider is the subject of an order made by the Court or tribunal for its compulsory winding-up or dissolution;
- (h) the virtual asset service provider engages in unsafe and unsound practices; or
- (i) a competent authority or comparable body makes a request for the suspension or revocation of the licence provided that upon receipt of the written request, the Bank conducts its own investigation.

Notice of intention to suspend or revoke licence

15. (1) Where the Bank decides to—

- (a) vary any condition to which the licence is subject or to impose a condition thereon; or
- (b) suspend or revoke a licence, the Bank shall give the virtual asset service provider 21 days' written notice of its intention to do so, setting out the reasons for the decision it proposes to take.

(2) A virtual asset service provider may, within 14 days after receipt of the notice given under sub-directive (1), make written representations to the Bank, stating reasons why the proposed decision should not be taken, and the Bank shall consider any representation so made before arriving at a final decision.

(3) The Bank may, where it is satisfied that the virtual asset service provider fulfills the requirements of these Directives, lift the suspension on such conditions as it may consider necessary, including varying any condition to which the licence is subject or imposing further conditions thereon.

Suspension or revocation of licence without notice

16. (1) Notwithstanding directive 15, the Bank may —

- (a) suspend a licence, without notice, where the Bank considers that an immediate suspension is necessary to protect the public; or
- (b) revoke a licence, without suspension, where the virtual asset service provider has voluntarily surrendered its licence.

(2) The Bank shall, as soon as is practicable, notify the virtual asset service provider of its decision, in writing.

Notification of revocation, winding up etc.

17. Where the Bank revokes a licence, the Bank shall—

- (a) notify comparable bodies and competent authorities of the revocation as may be necessary;
- (b) by notice in Gazette, notify the public of the revocation; and
- (c) where necessary, make a written request to a competent authority for immediate deregistration, dissolution or winding up of the virtual asset service provider.

Register of virtual asset service providers

18. (1) The Bank shall maintain, in such form and manner as may be determined, a register of virtual asset service providers.

(2) Notwithstanding the generality of sub-directive (1), the register shall state—

- (a) the full names and physical address of the virtual asset service provider;
- (b) the licence, in respect of the virtual asset services, held by a virtual asset service provider, including any licence issued, or registration by a comparable body with respect to the provision of virtual asset services;
- (c) virtual asset services provided by the virtual asset service provider;
- (e) any conditions imposed by the Bank on the virtual asset service provider or licence; and
- (f) any other information the Bank may consider necessary.

(3) The register kept in terms of sub-directive (1) shall be open for inspection to any member of the public.

(4) A virtual asset service provider to which an entry in the register relates, shall as soon as practicable after it becomes aware of any error in the entry or any change in circumstances that is likely to have a bearing on the accuracy of the entry, give notice in writing to the Bank of the error or change in circumstances.

Corporate Governance

19. (1) A virtual asset service provider shall comply with the Banking and Financial Services Corporate Governance Directives.

(2) Notwithstanding the generality of sub-directive (1) above, a virtual asset service provider must—

- (i) have and maintain effective, robust and well- documented corporate governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;

(ii) ensure shareholders, board members and senior management satisfy the fit and proper criteria prescribed by the Bank on an ongoing basis;

(iii) at a minimum have office bearers in the positions of or equivalent to Chief Executive Officer, Chief Financial Officer, Chief Operating Officer/Chief Information Technology Officer, Chief Risk Officer and Compliance Officer.

Acquisition of beneficial interest in a virtual asset service provider

20. (1) Subject to sub-directive (3), a person shall not without prior approval of the Bank, in writing—

(a) acquire any beneficial interest in the voting shares of a virtual asset provider; or

(b) enter into any voting arrangement or other agreement that would enable that person or another person to control more than twenty-five percent of the total votes that could be cast at a meeting of the virtual asset service provider.

(2) A request for approval made in terms of sub-directive (3) shall include sufficient information to enable the Bank to consider the proposed acquisition in relation to—

(a) the nature of the proposed acquisition;

(b) who the proposed beneficial owners and any person who has control or management of the beneficial owner; and

(c) how the proposed acquisition is to be financed.

(3) Where a person intends to—

(a) acquire beneficial interest in the voting shares of a virtual asset service provider; or

(b) enter into a voting arrangement, trust or other agreement; that would enable that person to control more than twenty-five percent of the total votes that may be cast on a resolution at a meeting of the virtual asset service provider, the virtual asset service provider shall obtain the prior written approval of the Bank.

(4) In assessing a proposed acquisition, the Bank shall have regard to—

(a) the likely influence of the proposed beneficial owner on the virtual asset service provider;

(b) the suitability of the proposed beneficial owner and the financial soundness of the proposed acquisition;

(c) documentary evidence of the acquisition being approved by the body responsible for authorising mergers and acquisitions in Zambia; and

(d) whether there are reasonable grounds to suspect that the acquisition is a suspicious transaction.

(5) Where a virtual asset service provider referred to in sub-directive (1) is publicly traded, the virtual asset service provider shall notify the Bank as soon as it becomes aware that a person has become a significant shareholder in the virtual asset service provider.

(6) The Bank shall, within sixty days of receipt of a request for approval as specified in sub-directive (3), grant or reject the request.

(7) Where the Bank rejects a request for approval, made in accordance with sub-directive (3), the Bank shall inform the requester, in writing, of the reasons for the rejection within fourteen days of such rejection.

(8) Sub-directive (1) does not apply to a company which has more than fifty-one percent of its shares publicly traded on a securities exchange, whether within Zambia or outside Zambia, acceptable to the Bank.

(9) A person that contravenes this directive commits an offence and is liable, upon conviction, to a fine not exceeding two thousand five hundred penalty units or to imprisonment for a term not exceeding two years, or to both.

PART III

OBLIGATIONS OF A VIRTUAL ASSET SERVICE PROVIDER

Transfer of virtual assets

21. (1) The obligations pertaining to the transfer of virtual assets shall be as determined by the Bank, and other applicable laws.

(2) Notwithstanding the generality of sub-directive (1), a virtual asset service provider undertaking a transfer relating to virtual assets equal to, or above, a prescribed threshold shall—

(a) identify and verify the identity of the originator;

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

- (c) obtain and maintain the account number of the originator and beneficiary, or in the absence of an account number, a unique reference number;
 - (d) obtain and maintain the originator's address or, in the absence of address, the national identity number, or date and place of birth; and
 - (e) include information from paragraphs (a) to (c) in the message or payment form accompanying the transfer.
- (3) A virtual asset service provider receiving virtual asset equal to, or above, a prescribed threshold shall—
- (a) identify and verify the identity of the beneficiary;
 - (b) obtain and maintain information on the identity of the originator;
 - (c) obtain and maintain the account number of the originator and beneficiary, or in the absence of an account number, a unique reference number; and
 - (d) obtain and maintain the beneficiary's address or, in the absence of address, the national identity number, or date and place of birth.

Custody and protection of customer assets

22. (1) A virtual asset service provider that has custody of one or more virtual assets for a customer shall—
- (a) maintain, in its custody, a sufficient amount of each type of virtual asset in order to meet the virtual asset service provider's obligations to the customer;
 - (b) put in place multi-user access requirements; and
 - (c) meet all financial requirements, as may be determined by the Bank.
- (2) The virtual asset referred to in sub-directive (1) shall—
- (a) be segregated from that of the virtual asset service provider;
 - (b) be held by the virtual asset service provider for the customer entitled to the virtual asset;
 - (c) not be the property or virtual asset of the virtual asset service provider; and
 - (d) not be subject to the claims of creditors of the virtual asset service provider.

(3) This directive shall not apply to the custody of virtual assets that constitute securities or investment instruments as defined under the Securities Act No. 41 of 2016, which are subject to the regulatory oversight of the Securities and Exchange Commission.

Systems and controls

23. A virtual asset service provider shall establish systems and controls that are adequate and appropriate for the scale and nature of the business activities, including systems and controls which adequately and appropriately address the—

- (a) recording, storing, protection and transmission of information;
- (b) effecting and monitoring of transactions;
- (c) operation of the measures taken for securing the timely discharge, whether by performance, compromise or otherwise, of the rights and liabilities of the parties to the transaction;
- (d) safeguarding and administration of virtual assets belonging to customers;
- (e) cybersecurity measures implemented on the platform; and
- (f) business continuity and planning, in the event of a disruption of a virtual asset service.

Segregation and protection of customer funds

24. (1) A virtual asset service provider shall open and maintain a collection account fundsor wallet at a bank, financial institution or e-money institution.

(2) The account opened under sub-directive (1), shall be a holding account opened on behalf of customers entitled to the funds.

(3) For any electronic value issued and outstanding in the virtual asset service provider's ecosystem, there should be an equivalent amount in the holding account held at a bank, financial institution or e-money institution.

4) The funds in the holding account shall not be—

- (a) commingled with the virtual asset service provider's operational funds; and
- (b) subject to the claims of creditors of the virtual asset service provider.

(5) A virtual asset service provider shall not hold more than 50 percent of the total customer funds in a single bank, financial institution or e-money institution.

(6) The virtual assets and electronic value held on the virtual asset service provider's or any other third-party platform on behalf of the customer of the virtual asset service provider shall not be subject to the claims of creditors of the virtual asset service provider or any third party.

Prohibition to use agents

25. A Virtual Asset Service Provider shall not use agents in the provision of virtual asset services, except for marketing purposes.

Mis-selling by agents

26. (1) Where a virtual asset service provider uses agents to market its business to the public, it must—

(i) ensure that the information is not misleading

(ii) provide the Agent with adequate ongoing training and supervision on activities relating to the provision of virtual asset services including:

(a) Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation financing;

(b) consumer protection;

(c) fraud prevention; and

(d) data protection.

(2) The Virtual Asset Service Provider shall submit to the Bank an annual report on the adequacy and frequency of such training.

PART IV

PROFESSIONAL CONDUCT AND COMPLIANCE OF VIRTUAL ASSET SERVICE PROVIDERS

Professional conduct of virtual asset service provider

27. A virtual asset service provider shall, in providing virtual asset services—

(a) act honestly and fairly;

(b) act with due care, skill and diligence;

(c) observe and maintain a high standard of professional conduct;

(d) ensure that appropriate measures are put into place for the protection of customers' virtual assets; and

(e) have effective corporate governance arrangements consistent with the Banking and Financial Services Corporate Governance Directives.

Audited financial statements

28. A virtual asset service provider shall submit to the Bank an audited financial statement not later than three months after the close of its financial year, in respect of all transactions related to the provision of virtual asset services.

Material change to business activities

29. (1) A virtual asset service provider shall apply, in writing, to the Bank for approval to—

(a) modify the scope of the virtual asset services to be provided;

(b) re-organise its legal structure;

(c) merge with another entity; or

(d) change its name.

(2) A virtual asset service provider shall not, without the approval of the Bank—

(a) expand the scope of its activities;

(b) merge with another entity;

(c) appoint a new director;

(d) add or reduce its shareholders; or

(e) change or modify its name.

PART V

ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION

Compliance with Anti-Money Laundering, Combating the Financing of Terrorism and proliferation

30. (1) A virtual asset service provider shall be required to undertake measures to prevent the use of their networks for purposes associated with money laundering, terrorism financing, and other financial crimes.

(2) A virtual asset service provider shall—

- (a) comply with the Prohibition and Prevention of Money Laundering Act, the Financial Intelligence Centre Act and relevant AML/CFTP laws and regulations;
- (b) designate an approved officer at senior management level to be responsible for reporting all transactions suspected of being related to money laundering, terrorism financing and proliferation;
- (c) have a robust risk management framework that takes into account anti-money laundering and countering financing of terrorism and proliferation financing; and
- (d) not invoke non-disclosure agreements, banking, professional or contractual secrecy as a pretext for refusing to perform their statutory reporting obligation in regard to suspicious activity.

Customer on-boarding

31. (1) A virtual asset service provider shall have a customer on-boarding policy that is approved by its Board.

(2) Subject to the Financial Intelligence Centre Act, a virtual asset service provider may accept the following identification documentation for the purposes of conducting customer due diligence when providing a virtual asset service:

- (a) National Registration Card;
- (b) valid passport;
- (c) valid driver's licence;
- (d) in the case of a person granted refugee status in accordance with the Refugees Act, a refugee identification card; or
- (e) other official, independent and verifiable identification documentation approved by the Bank.

(3) Prior to providing the virtual asset service, a virtual asset service provider shall carry out customer due diligence (CDD) in line with the National Payment Systems Act, the Banking and Financial Services Act, the Financial Intelligence Centre Act and the Bank of Zambia Anti-Money Laundering and Combating Financing of Terrorism or Proliferation Directives, 2017.

PART VI

OUTSOURCING

Outsourcing

32. (1) A virtual asset service provider wishing to outsource any important operational function relating to the offering of virtual asset services shall do so in line with the Bank of Zambia Guidelines on outsourcing.

(2) Notwithstanding the generality of sub-directive (1) above, a virtual asset service provider—

- (a) intending to outsource any important operational function relating to the offering of virtual asset services shall not do so without prior written approval from the Bank;
- (b) shall remain responsible and accountable for any services outsourced; and
- (c) shall take all necessary steps to conduct relevant due diligence on the third party.

(3) Where a virtual asset service provider intends to outsource an important operational function, the following conditions shall be met—

- (a) each outsourced arrangement shall be governed by a written agreement that is legally enforceable;
- (b) the outsourcing does not impair:
 - (i) the quality of the institution's internal controls;
 - (ii) the ability of the Bank to provide effective oversight of the activities of the virtual asset service provider;

- (iii) the ability of a virtual asset service provider to comply with these Directives and other relevant laws;
 - (c) outsourcing does not result in senior management delegating its responsibility to comply with the requirements imposed by these Directives;
 - (d) the relationship and obligations of the virtual asset service provider towards its customers under these Directives is not altered;
 - (e) compliance with the conditions under which the licence was issued will not be adversely affected; and
 - (f) none of the conditions of the institution's licence requires removal or variation.
- (4) For purposes of sub-directive 32(1), an operational function is important if a defect or failure in its performance would materially impair—
- (a) compliance by a virtual asset service provider with these Directives;
 - (b) the financial performance of the virtual asset service provider;
 - (c) the soundness or stability of the virtual asset service provider;
 - (d) quality of provision of virtual asset services which include;
 - (i) the rights and privileges of customers; and
 - (ii) customer support and redress mechanisms.
- (5) A person who contravenes this directive commits an offence and is liable to a fine not exceeding two thousand five hundred penalty units.

PART VII

CUSTOMER TRANSACTIONS AND PROTECTION

Complaint Management and Customer complaint handling procedures

33. (1) A virtual asset service provider shall ensure that—
- (a) its customer facing staff have an understanding of the service being offered;
 - (b) it discloses to customers the risks inherent in the virtual asset services on offer;
 - (c) a customer is made aware of the costs and commissions of the services before carrying out any transaction; and
 - (d) customer data and information is protected and kept confidential.
- (2) A virtual asset service provider shall—
- (a) have a framework for informing a customer on how to make a complaint. The minimum information to be disclosed shall include:—
 - (i) all available ways to lodge a complaint, including contacts for the recipient of the complaint;
 - (ii) description, in plain language, of the complaints handling process including guidelines on how to lodge a complaint;
 - (iii) information about maximum time limits to resolve a complaint; and
 - (iv) information about making an appeal to the Bank if not satisfied with the resolution by the virtual asset service provider.
 - (b) at a minimum, display the information in sub-directive 33(2)(a) above prominently in all branches, on its electronic sites including the virtual asset service provider's website, smart application or other electronic channels;
 - (c) explain the redress process at onboarding which must include but not be limited to:
 - (i) contact details of the help desk; and
 - (ii) escalation matrix where the customer is not satisfied with resolution of the virtual asset service provider.
 - (d) designate a senior officer or other employee to be a customer service officer responsible for implementing and administering the customer complaint procedures;
 - (e) maintain a record of customer complaints received indicating the nature of the complaint, when it was received and how the complaint was resolved or disposed of for a period of ten years.
- (2) A virtual asset service provider shall have a clear dispute management process that outlines at a minimum:
- (a) timelines and expected outcomes of each process;
 - (b) the dispute resolution shall be governed by Zambian Law; and
 - (c) escalation matrix and contact persons within the virtual asset service provider to address customer disputes.

Risk Management

34. (1) A virtual asset service provider shall maintain and enforce risk management processes, procedures, systems and controls to mitigate risks and safeguard customer funds.

(2) A virtual asset service provider shall establish effective procedures on risk detection, analysis, investigation and reporting, which shall include:

- (a) risk detection and transaction monitoring systems that can facilitate timely identification and mitigation of fraud risks; and
- (b) reporting of risk incidents to senior management, law enforcement agencies, and to the Bank.

(3) Where the Bank observes an escalating pattern of risks on a virtual asset service provider's platform, it may take necessary supervisory action including administratively penalising the institution.

(4) In the event of risk occurrences, a virtual asset service provider shall take appropriate and immediate corrective measures to redress affected customers and address gaps and vulnerabilities in order to strengthen the security controls.

(5) A virtual asset service provider that fails to comply with sub-directive 34(2), shall be liable to supervisory action including a fine of two thousand five hundred penalty units.

Consumer awareness on virtual asset services

35. (1) A virtual asset service provider shall sensitise its customers on virtual assets and safety measures expected during their use.

(2) A virtual asset service provider shall:

- (a) put in place an annual awareness plan for customers of virtual assets, which plan should be submitted to the Bank;
- (b) conduct awareness campaigns at-least twice a year; and
- (c) submit a report to the Bank on the outreach conducted, topics covered, key findings during awareness and measures the virtual asset service provider developed to address consumer concerns within three months of conducting the outreach.

Business Continuity

36. (1) A virtual asset service provider shall adopt an effective business continuity programme to mitigate disruption of its services.

(2) A virtual asset service provider shall develop and maintain a well-documented and tested business continuity and disaster recovery plan approved by its board.

(3) A business continuity plan shall at a minimum include:

- (a) a register of key contact persons and assignment of roles in the event of an incident;
- (b) ability to resume critical services within the defined recovery objectives, but not beyond 2 hours; and
- (c) frequency of testing which shall be quarterly and supported with evidence.

(4) A virtual asset service provider shall be required to provide evidence of routing transactions through its disaster recovery site during its quarterly business continuity test.

(5) A virtual asset service provider shall determine Recovery Point Objectives (RPO) and put in place procedures and mechanisms to minimise loss of data on critical systems.

(6) A virtual asset service provider shall determine appropriate recovery matrices such as Maximum Tolerable Downtime (MTD) and Recovery Time Objectives (RTO) for each critical business function.

(7) The Business Continuity Plan shall detail the procedures and the minimum level of resources required to recover the critical business functions within the recovery timeframe.

(8) A virtual asset service provider shall submit to the Bank, in a prescribed manner and form, a report on the quarterly Business Continuity test.

Data protection

37. (1) A virtual asset service provider shall implement and maintain, in relation to the protection of personal data relative to the customer, data protection measures consistent with the Data Protection Act, 2021.

(2) Notwithstanding the generality of sub-directive (1), a virtual asset service provider shall implement measures to protect data and preserve the confidentiality of information of customers through the entire life cycle of a transaction which shall include at a minimum:

- (a) outlined control measures to access data;
- (b) encryption and decryption mechanisms for data at rest, in transit and in use; and
- (c) procedures for storing customer transaction data.

(3) A virtual asset service provider that receives data in respect of a customer of another virtual asset service provider shall:

- (a) only use that data to comply with its obligations under these Directives;
- (b) treat the data as confidential information;
- (c) take all reasonable measures to protect the data against loss and unauthorised access, use, disclosure or modification; and

(d) ensure that any person who is given access to the data is made aware of and undertakes to comply with the obligations in these Directives.

(4) A virtual asset service provider must have mechanisms which enable the monitoring of attempted security breaches that may compromise its systems and data.

(5) A virtual asset service provider that develops, uses or provides an application programming interface shall establish safeguards that meet international standards to manage the development and provision of the application programming interfaces to secure the interaction and exchange of data between various software applications.

(6) A virtual asset service provider shall not store customer data within its database or the servers in an unencrypted format.

Cybersecurity

38. (1) A virtual asset service provider shall comply with the Cyber Security Act, Electronic Communications and Transactions Act, and the Bank of Zambia Cyber and Information Risk Management Guidelines.

(2) Notwithstanding the generality of sub-directive (1), a virtual asset service provider shall:

(a) protect its infrastructure, network, data and systems against cyber attacks;

(b) put in place measures to mitigate all forms of security risks, particularly cyber risks;

(c) develop appropriate security policies and measures to safeguard the confidentiality, integrity and availability of data, and operating processes;

(d) set minimum end-to-end data encryption standards;

(e) ensure that any data stored in third party systems is secured with appropriate encryption and hardware security standards;

(f) undertake annual penetration testing and vulnerability assessments; and

(g) undertake annual security audits to assess information security practices and controls to identify vulnerabilities, weaknesses and potential risks.

(3) The Board, or a committee designated by the Board, shall be responsible for ensuring that an enterprise risk management framework is established and maintained to manage operational and cyber security risks.

4) A virtual asset service provider shall, within 48 hours, report the occurrences of cyber-incidents to the Bank, and these may be shared with other regulated entities.

(5) The Bank shall determine the manner and form in which Cyber incidents shall be reported and shared.

Disclosure of charges

39. A virtual asset service provider shall disclose its transaction charges to the customer—

(a) electronically at the point of transacting prior to the customer completing the transaction where the charge is dependent on the transaction value; and

(b) through websites, smartphone applications or other electronic channels as a supplementary measure.

(2) A virtual asset service provider shall apply to the Bank for approval of all charges before they are implemented or adjusted.

(3) The Bank may approve or reject the application by the virtual asset service provider to adjust the charges.

PART VIII

RECORDS AND RETURNS

Retention of Records

40. A virtual asset service provider shall retain customer information and transaction records for a minimum period of ten years from the date on which the record was created.

Returns and information

41. (1) A virtual asset service provider shall submit returns to the Bank in the manner and form determined by the Bank.

(2) A virtual asset service provider shall submit an incident report to the Bank within 48 hours of all major incidents affecting its operations. The report shall state controls in place and steps taken to rectify the matter and prevent reoccurrence.

(3) The Bank may require a virtual asset service provider to submit any other information that it may consider necessary such as taxpayer identification number of transacting resident parties.

Request for information

42. (1) The Bank may, by notice in writing, require a person to furnish to the Bank, at such time and place and in such form as may be determined, information and documentation, with respect to—

- (a) a virtual asset activities;
 - (b) a beneficial owner of a virtual asset service provider.
- (2) A person in sub-directive (1), may include—
- (a) any person who is, was or appears to be or to have been, a virtual asset service provider;
 - (b) an agent of a virtual asset service provider; or
 - (c) an intermediary involved in a virtual asset service or any other person that the Bank may deem necessary.
- (3) The Bank may request a virtual asset service provider to appear before it or a person appointed by the Bank, at such time and place as it may specify, to answer questions and provide information and documentation with respect to a virtual asset or virtual asset service.

PART IX

EXAMINATION AND INVESTIGATION

Examination

43. (1) The Bank may cause an examination to be made of a virtual asset service provider in order to determine whether the service provider is—
- (a) in a sound financial condition; and
 - (b) complying with these Directives, and any other relevant written law.

Investigation

44. (1) The Bank may, by the Bank's employees or agents, investigate the activities or operations of a virtual asset service provider in line with the Act.
45. (1) A virtual asset service provider shall provide such information as may be required by the Bank for the purpose of monitoring the institution's compliance with these Directives and any other relevant regulations.
- (2) A virtual asset service provider shall allow the Bank to carry out on-site examinations at—
- (a) the premises of a virtual asset service provider, its branch or designated location;
 - (b) the premises of any entity to which a virtual asset service provider's activities are outsourced.
46. The Bank may cooperate with relevant institutions in conducting oversight or investigations of virtual asset service providers.

PART X

GENERAL PROVISIONS

General offences and penalties

47. (1) A virtual asset service provider that contravenes these Directives commits an offence and is liable upon conviction to a fine not exceeding two thousand five hundred penalty units, or imprisonment for a term not exceeding two years, or to both.
- (2) A Virtual Asset Service Provider that—
- (a) willfully makes any misrepresentation in any document required to be submitted under these Directives; or
 - (b) willfully makes any statement or gives any information required for the purpose of these Directives which the person knows to be materially false or misleading; or
 - (c) knowingly fails to disclose any fact or information required to be disclosed for the purposes of these Directives, commits an offence and is liable, upon conviction, to a fine not exceeding two thousand five hundred penalty units, or to imprisonment for a term not exceeding two years or to both.
- (3) A person who destroys, falsifies, conceals or disposes of, or causes or permits the destruction, falsification, concealment or disposal of, any document, information stored on a computer or other device or other thing that the person knows or ought reasonably to know is relevant to the Bank, commits an offence and is liable, upon conviction, to a fine not exceeding two thousand five hundred penalty units or to imprisonment for a term not exceeding two years, or to both.
- (4) Where an offence has been committed under these Directives and it is proved that the offence occurred with the consent, knowledge, connivance or gross negligence of a director or senior officer of the Virtual Asset Service Provider, or any person purporting to act in any such capacity, each such person commits an offence and is liable to the same penalty as provided for under these Directives.

Administrative sanctions

48. (1) The Bank may, where the Bank is satisfied after due investigation or where a person admits that the person has committed an offence in terms of the Act, these Directives, or regulatory statements issued by the Bank, compound the offence and impose an administrative penalty, as may be determined.

(2) The Bank may, where a person on whom an administrative penalty is imposed under sub-directive 48(1) fails to pay the penalty within a period the Bank may specify, recover the penalty by action in a court of competent jurisdiction.

Insolvent virtual asset service provider

49. (1) In these Directives, “insolvency event” means any of the following procedures in relation to a virtual asset service provider—

- (a) the making of a winding-up order;
- (b) the passing of a resolution for voluntary winding-up;
- (c) the entry of the institution into administration;
- (d) the appointment of a receiver or manager of the institution’s property;
- (e) the approval of a proposed voluntary arrangement (being a composition in satisfaction of debts or a scheme of arrangement);
- (f) the making of a bankruptcy order;
- (g) the making of an insolvency administration order; or
- (h) the conclusion of any composition contract with creditors.

(2) In an insolvency event, a virtual asset service provider shall not enter into any new or continue to conduct any existing virtual asset service except that which is incidental to the orderly realisation, conservation and preservation of its assets.

External Auditors

50. (1) A virtual asset service provider shall appoint an external auditor who shall be a member in good standing of a professional body of accountants in Zambia.

(2) A virtual asset service provider shall be required to submit to the Bank a copy of auditor’s opinion, together with a copy of the audited annual financial statement within a period of three months from the end of each financial year.

(3) The Bank may appoint an external auditor or any other subject matter expert at the expense of a virtual asset service provider to conduct a special audit relating to the operations of the service provider.

Appeals against decisions of the Bank

51. A person who is aggrieved by the decision of the Bank made in accordance with the provisions of these Directives, may appeal such decision to the Tribunal established under the Act.

Transitional provisions

52. Where, on the commencement of these Directives, a person is providing a virtual asset service, the person shall make an application in such manner as may be determined, not later than twelve months after the commencement of these Directives, to be licensed as a virtual asset service provider.

Exemptions

53. The Bank may on such terms and conditions as may be determined exempt, waive or vary the application of any of these Directives.

Commencement date

54. These Directives shall come into force on the day that they are published in the *Gazette*.

LUSAKA

18th September, 2026

F. CHIPIMO,
Deputy Governor-Operations