

EXTRAORDINARY

OFFICIAL GAZETTE
THE BAHAMAS

PUBLISHED BY AUTHORITY

NASSAU 27th October, 2026

DIGITAL ASSETS AND REGISTERED EXCHANGES (ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTERING FINANCING OF PROLIFERATION) RULES, 2026

Arrangement of Rules

Rule

PART I - PRELIMINARY **3**

1. Citation....3
2. Interpretation....3

PART II - RISK RATING DUTY OF REGISTRANT **6**

3. Duty of registrant to implement risk rating framework....6

PART III - INTERNAL CONTROLS **9**

4. Duty of registrant concerning internal controls....9
5. Group-wide programmes....9
6. Money laundering reporting officer....10
7. Outsourcing of MLRO services....10
8. Suspicious transaction reporting....11
9. Outsourcing and third-party technology service providers. 12
10. Mandatory initial and ongoing due diligence of third-party technology service providers. 12
11. Requirements for outsourcing and third-party technology arrangements....13

PART IV - VERIFICATION OF CUSTOMER IDENTITY **13**

12. Due diligence measures....13
13. Simplified due diligence measures....14
14. Enhanced due diligence measures....15
15. Verification of customer identity....16
16. Use of a business relationship prior to completion of verification....17
17. Required information....18
18. Politically exposed persons....22
19. Reliance on third party verification procedures....24
20. Eligible introducer....24
21. Suspension or termination of activity or business....25
22. Simplified verification for specified customers....26
23. Ongoing monitoring....27

PART V — TRANSFERS OF DIGITAL ASSETS **27**
24. Transfers of digital assets....27
25. Counterparty institutions....29
26. Transfers involving unhosted wallets....29

PART VI – TARGETED FINANCIAL SANCTIONS **30**
27. Targeted financial sanctions....30

PART VII - RECORD KEEPING **30**
28. Maintenance of records....30
29. Transaction records....31
30. Other records....32

PART VIII - MISCELLANEOUS **32**
31. Education and training....32
32. Revocation of S.I. No. 32 of 2022....33



MINISTRY OF FINANCE

S.I. No. 104 of 2026

DIGITAL ASSETS AND REGISTERED EXCHANGES ACT, 2024
(NO. 40 OF 2024)

DIGITAL ASSETS AND REGISTERED EXCHANGES (ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTERING FINANCING OF PROLIFERATION) RULES, 2026

The Securities Commission of The Bahamas, in exercise of the powers conferred by section 80 of the Digital Assets and Registered Exchanges Act, 2024 makes the following rules —

PART I - PRELIMINARY

1. Citation.

These Rules may be cited as the Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering the Financing of Terrorism and Countering Financing of Proliferation) Rules, 2026.

2. Interpretation.

(1) In these Rules —

"Act" means the Digital Assets and Registered Exchanges Act, 2024 *(No. 40 of 2024)*;

"AML/CFT/CPF" means anti-money laundering, countering the financing of terrorism and countering financing of proliferation;

"Anti-Terrorism Act" means the Anti-Terrorism Act, 2018 *(No. 27 of 2018)*;

"beneficial owner" has the meaning assigned to it under section 2 of the Financial Transactions Reporting Act;

"beneficiary" means the natural person, legal person or legal arrangement identified by the originator as the receiver of a transfer of digital assets;

"beneficiary institution" means the registrant, virtual asset service provider or financial institution which receives a transfer of digital assets from an ordering institution or an intermediary institution and makes the digital assets available to the beneficiary;

"Commission" means the Securities Commission of The Bahamas continued under section 10 of the Securities Industry Act;

"counterparty institution" means the ordering institution, intermediary institution or beneficiary institution with which a registrant interacts in connection with a transfer of digital assets;

"**customer**" has the meaning assigned to it under section 2 of the Financial Transactions and Reporting Act, and where the context requires includes client or facility holder;

"designated person or entity" means a designated entity as defined under section 2 of the Anti-Terrorism Act;

"digital assets" has the meaning specified under section 2 of the Act;

"**facility holder**" has the meaning assigned to it under the Financial Transactions and Reporting Act;

"financial group" means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with the branches and subsidiaries of the group that are subject to AML/CFT/CPF policies and procedures at the group level;

"financial institution" has the meaning specified under section 3 of the Financial Transaction Reporting Act;

"financing of proliferation" means the financing of proliferation of weapons of mass destruction specified under section 9 of the Anti-Terrorism Act;

"Financial and Corporate Service Providers Act" means the Financial and Corporate Service Providers Act, 2020 *(No.27 of 2020)*;

"Financial Transactions Reporting Act" means the Financial Transactions Reporting Act, 2018 *(No. 5 of 2018)*;

"Financial Transactions Reporting (Wire Transfers) Regulations" means the Financial Transactions Reporting (Wire Transfers) Regulations, 2018 *(S.I. No. 36 of 2018)*;

"identified risk" has the meaning assigned to it under section 2 of the Financial Transaction Reporting Act;

"intermediary institution" means the registrant, virtual asset service provider or financial institution which, in a transfer of digital assets, receives and retransmits the digital assets on behalf of the ordering institution and the beneficiary institution, or on behalf of another intermediary institution;

"International Obligations (Economic and Ancillary Measures) Act" means the International Obligations (Economic and Ancillary Measures) Act *(Ch. 16)*;

"key personnel" means senior management or other key employees who effectively manage the business of a registrant;

"Money Laundering Reporting Officer" or **"MLRO"** means a person appointed by a registrant as its Money Laundering Reporting Officer in accordance with rule 6;

"occasional transactions" has the meaning assigned to it under section 2 of the Financial Transactions Reporting Act;

"ordering institution" means the registrant, virtual asset service provider or financial institution which initiates a transfer of digital assets on behalf of the originator;

"originator" means the natural person, legal person or legal arrangement on whose behalf a transfer of digital assets is initiated;

"registrant" means a person registered under the Act;

"Securities Industry Act" means the Securities Industry Act, 2024 *(No. 39 of 2024)*;

"senior management" means an officer or employee of a registrant with sufficient knowledge and seniority to make decisions affecting the registrant's risk exposure and need not involve a member of the board or directors and includes a person responsible for compliance or duly authorised to bind the registrant;

"suspicious transaction report" means a report made pursuant to section 25 of the Financial Transactions Reporting Act;

"targeted financial sanctions" means sanctions imposed against a person or entity pursuant to section 3A of the International Obligations (Economic and Ancillary Measures) Act, to freeze or restrain money, assets or property and any prohibition on making money, assets or property available, directly or indirectly, to or for the benefit of that person or entity;

"transfer of digital assets" means a transaction carried out on behalf of an originator with a view to making a digital asset available to a beneficiary at a beneficiary institution or at an unhosted wallet, irrespective of whether the originator and the beneficiary are the same person; and

"virtual asset service provider" means a person, wherever located, who carries on any activity which, if carried on in or from within The Bahamas, would constitute digital asset business under the Act.

(2) In these Rules, references to "money laundering, financing of terrorism and financing of proliferation" or "AML/CFT/CPF", where used in relation to the assessment, management or mitigation of risk, shall be construed to include all identified risk as defined under section 2 of the Proceeds of Crime Act.

(3) These Rules are in addition to, and do not derogate from, any obligation of a registrant or of any other person under the Financial Transactions Reporting Act, the Anti-Terrorism Act, the International Obligations (Economic and Ancillary Measures) Act or any other enactment concerning money laundering, financing of terrorism and financing of proliferation.

PART II - RISK RATING DUTY OF REGISTRANT

3. Duty of registrant to implement risk rating framework.

(1) A registrant shall implement a risk rating framework which assesses and identifies —

(a) the risk profile of each customer;

(b) the registrant's risk profile in relation to the countries or jurisdictions in which it operates;

(c) the risk profile associated with the registrant's business practices, products, services, transactions and delivery channels;

(d) the nature and extent of risks related to the registrant’s non-face-to-face business relationships; and

(e) the nature and extent of risks related to the registrant’s business activities that permit customers to receive payments from unknown or unassociated third parties.

(2) The risk rating framework shall be approved by the registrant’s senior management based on the scope of the registrant's activities, and shall be designed to —

(a) take appropriate measures to continuously identify, measure, manage, and mitigate identified current and emerging risks;

(b) take account of any risk assessment carried out at the national level and any regulatory guidance issued by the Commission;

(c) categorise customer relationships and products to identify the level of risk associated with each customer relationship or product;

(d) categorise customer relationships and products to take account of risk factors related to the particular customer relationship or product, including —

(i) customer type or profession;

(ii) country of domicile;

(iii) complexity of ownership;

(iv) complexity of legal structure;

(v) source of business;

(vi) type of assets;

(vii) type, size and volume of transactions;

(viii) level of cash transactions;

(ix) non-face-to-face Know Your Customer document submission; and

(x) adherence to customer activity profile;

(e) address which level of management can approve a decision for the registrant to enter into customer relationships at the various levels of risk rating categories;

(f) establish Know Your Customer and due diligence information requirements appropriate for the risk profile of the customer relationship or product; including simplified due diligence and enhanced due diligence procedures;

(g) require the periodic review of the customer relationship or product to —

(i) ensure that the categorisations are current and appropriate; and

(ii) enable the registrant to determine whether any adjustment should be made to the risk rating;

(h) require the re-categorisation of a customer relationship or product offered by the registrant in the event of a change in the risk profile of a customer relationship or product;

(i) require the documentation of the basis for the risk rating applied to a customer relationship or product and of any changes in the risk rating of particular customer relationship or product;

(j) mitigate any additional risks due to the cross-border nature of a transaction, particularly where the transaction takes place in a jurisdiction which could reduce the registrant's ability of oversight and the application of effective anti-money laundering, countering the financing of terrorism and countering the financing of proliferation controls;

(k) identify and mitigate potential risks arising from products, services or activities, provided to or by anonymous or private sources including, but not limited to, unhosted wallets, the darknet and blacklisted addresses, particularly where the risk rating is high or where the type, size and volume of transactions is substantial.

(3) A registrant shall assess the risk profile of each new customer and carry out a risk assessment of each new product, business practice or technology before establishing a business relationship with such customer or introducing such product, business practice or technology.

(4) The outcome of each customer or product risk assessment conducted shall be documented and retained as part of the registrant's document keeping requirements.

(5) A registrant's risk rating framework shall be subject to review by the Commission.

PART III - INTERNAL CONTROLS

4. Duty of registrant concerning internal controls.

(1) A registrant shall implement internal control policies and procedures for the prevention, detection, and disclosure of activity related to identified risks, in accordance with the Financial Transactions Reporting Act and —

(a) document and track financial crime typologies specific to digital assets;

(b) have a MLRO approved by the Commission; and

(c) verify, on a regular basis, compliance with internal policies, procedures, and controls relating to identified risks.

(2) A registrant shall comply with the provisions of the Financial Transactions Reporting (Wire Transfers) Regulations, and ensure proper internal controls are in place.

(3) A registrant shall ensure it understands its operating processes and procedures, regularly verifies their integrity, and accounts for identified risks.

5. Group-wide programmes.

(1) A registrant that is a member of a financial group shall implement group-wide programmes against money laundering, the financing of terrorism and the financing of proliferation which are applicable and appropriate to all branches and majority-owned subsidiaries of the financial group, and shall include —

(a) the internal control policies and procedures required under rule 4;

(b) policies and procedures for sharing information within the financial group where required for the purposes of customer due diligence and the management of money laundering, financing of terrorism and financing of proliferation risk;

(c) the provision, to group-level compliance, audit and anti-money laundering, countering the financing of terrorism and countering the financing of proliferation functions —

(i) of customer, account and transaction information from branches and subsidiaries where necessary for those purposes, including information and analysis of transactions or activities which appear unusual; and

(ii) where relevant to the management of risk, the fact that a suspicious transaction report or its underlying information has been submitted;

(d) the provision by the group-level functions referred to under subparagraph (c), to branches and subsidiaries, of the information referred to under that subparagraph where relevant and appropriate to the management of risk; and

(e) adequate safeguards on the confidentiality and use of information exchanged within the financial group, including safeguards to prevent tipping-off.

(2) Where a registrant has a branch or majority-owned subsidiary in another country, the registrant shall ensure that the branch or subsidiary applies—

(a) measures consistent with these Rules and the Financial Transactions Reporting Act to the extent that the laws of that country permit; and

(b) where the laws of that country prevent the application of those measures, apply appropriate additional measures to manage the risks and inform the Commission of the same.

6. Money laundering reporting officer.

(1) A Money Laundering Reporting Officer —

(a) may be an individual or entity who complies with section 35(1) of the Act;

(b) if a legal person, is approved under the Financial and Corporate Service Provider Act to provide outsourced services as a MLRO.

(2) A registrant shall submit the name of the person proposed to be the MLRO to the Commission, and where the person is approved and appointed as the MLRO, the registrant shall —

(a) register the name of the person with the Financial Intelligence Unit;

(b) ensure that the MLRO or any person appointed to assist the MLRO has timely access to systems, customer records and relevant information required to perform their duties; and

(c) submit a statement that the MLRO is a fit and proper person.

7. Outsourcing of MLRO services.

(1) A registrant may outsource the role of the MLRO.

(2) Before outsourcing, the registrant shall —

(a) notify the Commission of the particulars and regulatory status of the proposed MLRO, including whether that person is an employee of a parent company or a company affiliated with the registrant;

(b) satisfy the Commission that the proposed MLRO has the relevant qualifications, knowledge, experience, managerial resources and operational capacity to meet the obligations of a MLRO; and

(c) provide the Commission with a copy of the executed outsourcing contract with the MLRO.

(3) The outsourcing arrangement must permit the Commission access to any records and information held by the MLRO relating to the activities carried out in relation to the registrant, as if those records and information were held by the registrant.

(4) Notwithstanding paragraph (1), a registrant shall retain ultimate responsibility for ensuring compliance with the provisions of the Financial Intelligence (Transactions Reporting) Regulations.

(5) The Commission may, by notice to the registrant, object to the proposed appointment or to the continued use of a MLRO and the registrant shall terminate the appointment promptly after receipt of such notice from the Commission.

8. Suspicious transaction reporting.

(1) A registrant shall implement policies and procedures to facilitate an employee exercising their duty to report their knowledge or suspicions that a customer is or may be engaged in money laundering or the financing of terrorism or the financing of proliferation to the MLRO.

(2) It shall be the responsibility of the MLRO to assess the sufficiency of the information contained in a report referred to under paragraph (1).

(3) The policies and procedures referred to under paragraph (1) shall extend to knowledge or suspicion arising in relation to attempted or proposed transactions and completed transactions.

(4) The MLRO shall promptly assess each report referred to under paragraph (1) promptly and, where the MLRO knows, suspects or has reasonable grounds to suspect that a transaction or proposed transaction involves the proceeds of criminal conduct, money laundering, the financing of terrorism or the financing of proliferation, shall ensure that a suspicious transaction report is filed with the Financial Intelligence Unit in accordance with the Financial Transactions Reporting Act.

(5) In establishing and operating its systems for the detection of suspicious transactions and suspicious activity, a registrant shall have regard to —

(a) indicators of suspicious activity;

(b) the financial crime typologies documented and tracked under rule 4(1)(a); and

(c) any guidance concerning the detection or reporting of suspicious transactions issued by the Commission or the Financial Intelligence Unit,

and shall incorporate relevant indicators into its transaction monitoring systems and into the education and training provided under rule 31.

9. Outsourcing and third-party technology service providers.

(1) A registrant may outsource operational, technical, or compliance functions to a third-party technology provider, provided that the registrant retains ultimate legal responsibility and liability for full compliance with all applicable anti-money laundering, countering the financing of terrorism and countering the financing of proliferation and regulatory obligations.

(2) No outsourcing arrangement, contractual agreement, or technology failure shall relieve the registrant, its board of directors, or its senior management of their legal duties, regulatory liabilities, or statutory penalties.

10. Mandatory initial and ongoing due diligence of third-party technology service providers.

(1) A registrant shall, before entering into any arrangements with a third-party technology provider for critical or regulated functions, conduct and document a comprehensive due diligence assessment of that third-party provider and evaluate, at a minimum —

(a) the vendor’s technical capabilities, system reliability, operational resilience, and cybersecurity controls;

(b) the vendor’s regulatory status and the anti-money laundering, countering the financing of terrorism and countering the financing of proliferation standards of the jurisdiction in which the vendor operates or stores data;

(c) the vendor’s financial stability, market reputation, and ownership structure; and

(d) potential conflicts of interest or concentration risks arising from reliance on the vendor.

(2) A registrant shall review and update its vendor due diligence assessments at least annually or immediately upon any material change in the service provider's operations or regulatory status.

11. Requirements for outsourcing and third-party technology arrangements.

(1) A registrant shall comply with the requirements specified in a policy published by the Commission in relation to the outsourcing of operational, technical or compliance functions and the use of third-party technology service providers, including requirements concerning —

(a) the assessment of risks associated with an arrangement and the conduct, documentation and review of initial and ongoing due diligence on the service provider;

(b) written contractual arrangements, including rights of access to information and records, inspection and audit rights for the registrant, its independent auditors and the Commission, data protection and security, and controls over subcontracting;

(c) the timely availability and retrieval of customer due diligence information, transaction information and supporting records by the registrant and the Commission;

(d) prior notification to the Commission of proposed material outsourcing arrangements or material changes to existing arrangements, together with the submission of supporting information;

(e) notification of cybersecurity breaches, system failures and regulatory non-compliance affecting outsourced functions; and

(f) the preparation, maintenance and testing of business continuity and disaster recovery plans, and documented exit strategies, including arrangements for data migration and the continuity of compliance functions.

(2) The policy referred to under paragraph (1), shall specify the arrangements to which the requirements apply and the applicable review periods, notification and submission timelines, and manner of compliance.

PART IV - VERIFICATION OF CUSTOMER IDENTITY

12. Due diligence measures.

(1) Except where specifically exempted by any Rules issued by the Commission, the customer due diligence measures implemented by the registrant shall use independent and reliable source documents, data or information (whether or not electronically sourced).

(2) The risk rating framework of a customer shall be applied by a registrant to its due diligence measures.

(3) Once a business relationship has been established with a customer, the registrant shall take reasonable steps to ensure that due diligence measures are periodically reviewed and kept up to date.

(4) A registrant shall apply customer due diligence measures to customers with which it has an existing business relationship on the basis of materiality and risk, and shall conduct due diligence on such existing relationships at appropriate times, taking into account —

(a) whether and when customer due diligence measures were previously undertaken; and

(b) the adequacy of the documents, data and information previously obtained.

13. Simplified due diligence measures.

(1) A registrant may apply simplified due diligence measures to a customer, business relationship or transaction only where —

(a) the registrant has assessed the risk of money laundering, the financing of terrorism and the financing of proliferation associated with the customer, business relationship or transaction as low in accordance with its risk rating framework under rule 3;

(b) there is no suspicion of money laundering, the financing of terrorism or the financing of proliferation; and

(c) no higher risk circumstance of the kind referred to under rule 14 or section 13 of the Financial Transactions Reporting Act applies.

(2) A registrant shall —

(a) document the basis for determining that a customer, business relationship or transaction presents a lower risk, together with the simplified due diligence measures applied; and

(b) comply with any direction issued by the Commission not to apply, or to cease applying, simplified due diligence measures.

(3) Where a registrant knows or suspects money laundering, the financing of terrorism or the financing of proliferation, or where the risk associated with the customer, business relationship or transaction is no longer low, the registrant shall —

(a) cease to apply simplified due diligence measures; and

(b) apply the due diligence measures otherwise required by these Rules.

14. Enhanced due diligence measures.

(1) Enhanced due diligence measures shall be applied by a registrant for categories of customers, business relationships, or transactions that may present a higher risk for activity related to identified risks based on the risk profile developed relative to the customer, business relationship or transaction, which measures shall include taking additional verification measures.

(2) A customer may present a higher risk for activity related to identified risks if, without limitation, a customer —

(a) is involved in digital asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk digital assets including, without limitation, those with anonymity enhancing features, or where its organisation gives rise to higher risk;

(b) is unable to produce the required Know Your Customer information and documentation;

(c) uses anonymous or randomly generated email addresses or a temporary email service;

(d) requests an exchange to or from cash or other digital assets with anonymity enhancing features;

(e) persistently avoids Know Your Customer thresholds through smaller transactions;

(f) requests an exchange to or from state-sponsored digital assets that are suspected of being used to avoid sanctions;

(g) is a politically exposed person as defined under rule 18;

(h) is from or established in, or is a party to a transaction connected with, a jurisdiction assessed by the IRF Steering Committee pursuant to section 13(1) of the Financial Transactions Reporting Act.

(3) A transaction may present a higher risk for activity related to identified risks if, without limitation —

(a) it is a peer-to-peer transaction;

(b) a significant proportion of the digital assets held or used in a transaction is associated with anonymity enhancing features or products and services that potentially obfuscate transactions or undermine a registrant's ability to know its customers and implement effective anti-money laundering, countering the financing of terrorism and countering the financing of proliferation controls;

(c) the digital asset comes from, or is associated with, the darknet or other illegal or high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes or sanctioned digital asset addresses or accounts;

(d) the results of blockchain analysis or similar analysis indicate a higher risk.

(4) Enhanced due diligence measures may include —

(a) corroborating the identity information received from the customer with information in third party databases or other reliable sources;

(b) for non-face to face Know Your Customer verification —

(i) video conferencing with the proposed customer;

(ii) requiring identification documentation to be certified by a notary public or the equivalent;

(iii) verifying with the customer, additional aspects of their identity (or biometric data) which is held electronically;

(c) tracing the customer's IP address;

(d) corroborating activity information consistent with the customer's transaction profile;

(e) obtaining additional information on the source of funds and source of wealth of the customer;

(f) obtaining information on the reasons for the intended or performed transaction;

(g) enhanced monitoring of the business relationship and transactions;

(h) requesting data relating to transaction and trading history.

15. Verification of customer identity.

(1) A registrant shall not enter into a business relationship or execute an occasional transaction with any person without applying customer due diligence measures to verify the identity of the person, including any beneficial owner.

(2) When verifying the identity of a person referred to under paragraph (1), the registrant shall —

(a) satisfy itself that the prospective customer is who the customer claims to be by applying the customer due diligence measures referred to under rules 12 to 14;

(b) ensure that sufficient information is obtained and documented —

(i) on the nature and purpose of the business that the customer intends to undertake; and

(ii) concerning any expected or predictable volume and pattern of transactions and activities; and

(c) satisfy itself that any independent and reliable source documents, data or information (whether or not electronically sourced) sufficiently verifies a customer's identity.

(3) Where a prospective customer fails or is unable to provide adequate evidence of identity, or a registrant is not satisfied that a new transaction with an existing customer is legitimate, the registrant shall —

(a) determine whether —

(i) other steps should be taken to verify the customer's identity;

(ii) it is appropriate to proceed or continue with the business relationship; and

(b) file a suspicious transaction report with the Financial Intelligence Unit.

(4) A registrant shall have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

(5) When verifying the identity of a customer, a registrant shall only accept —

(a) original documents;

(b) certified copies of documents from a prospective customer where submission of original documents is impractical or impossible;

(c) independent and reliable source documents, data or other information (whether or not electronically sourced) which sufficiently verifies a customer's identity; or

(d) photographed or scanned copies of identifying documents provided that the registrant has adequate internationally recognised tools to verify the authenticity of the documents.

(6) Notwithstanding any provision of these Rules, a registrant shall in any case verify the identity of a customer, prospective or existing, where the registrant knows or suspects activity related to identified risks and where such suspicion or knowledge is confirmed, shall make a report to the Financial Intelligence Unit.

16. Use of a business relationship prior to completion of verification.

(1) For the purposes of section 8(3) of the Financial Transactions Reporting Act, a registrant may complete the verification of the identity of a customer or beneficial owner after the establishment of the business relationship only where —

(a) deferral of the verification is essential in order not to interrupt the normal conduct of business;

(b) the verification is completed as soon as reasonably practicable after the establishment of the business relationship; and

(c) the risks of money laundering, the financing of terrorism and the financing of proliferation are effectively managed in accordance with paragraph (2).

(2) A registrant that permits a customer to utilise a business relationship before the completion of verification shall adopt risk management procedures specifying the conditions under which the customer may do so, which shall include —

(a) limits on the number, types or amount of transactions that may be performed before the completion of verification; and

(b) the monitoring of large or complex transactions carried out outside the expected norms for that type of relationship.

(3) Where the verification is not completed within a reasonable period, the registrant shall suspend activity on the account under rule 21, and shall determine whether it is appropriate to continue the business relationship, and shall consider whether a suspicious transaction report should be filed with the Financial Intelligence Unit.

17. Required information.

(1) A registrant shall obtain independent and reliable source documents, data or other information (whether or not electronically sourced) appropriate to the nature and structure of the proposed customer when verifying the proposed customer's identity, which shall include in the case of —

(a) a natural person —

(i) full and correct name(s);

(ii) at least two current means of contact which may include —

(aa) personal email address;

(bb) business email address;

(cc) personal mobile telephone number;

(dd) personal landline number;

(ee) business landline number;

(ff) personal mailing address, which must include where applicable, the street, post office box number, city, state or province, postal or zip code, landline telephone contact, and country;

(gg) business mailing address, which must include where applicable, the street, post office box number, city, state or province, postal or zip code, landline telephone contact, and country;

(hh) residential mailing address, which must include where applicable the street, post office box number, city, state or province, postal or zip code, landline telephone contact, and country; or

(ii) any specific means of contact which the Commission may specify;

(iii) date of birth;

(iv) country of domicile; and

(v) the purpose of the account and nature of the business relationship;

(b) a corporate customer —

(i) the original or a certified copy of the certificate of incorporation, registration or the equivalent;

(ii) certificate of good standing or the equivalent evidence that the company has not been or is not about to be struck off the register or wound up;

(iii) a copy of the relevant board resolution authorising the establishment of the business relationship, or authorising the opening of an account and conferring permission on any person authorised to undertake transactions;

(iv) satisfactory evidence of the identity of all persons authorised to undertake transactions and details of their relationship with the company; and

(v) satisfactory evidence of identification of each natural person having a beneficial interest of ten percent or more of the company, or having principal control over the company's assets or otherwise exercising control over the management of the company;

(c) a partnership or unincorporated business —

(i) a copy of the partnership agreement or document establishing the partnership agreement, or document establishing the partnership or unincorporated business;

(ii) a mandate authorising the establishment of the business relationship or the opening of an account, and conferring

permission on any person authorised to undertake transactions;

(iii) satisfactory evidence of the identity of partners and controllers of the firm or business; and

(iv) satisfactory evidence of the identity of persons authorised to undertake transactions;

(d) other legal structures and fiduciary arrangements, such as trusts, fiduciary or nominee structures —

(i) the applicable documents establishing the legal structure or fiduciary or nominee arrangement;

(ii) the applicable documents, identifying persons exercising effective control over the legal structure or fiduciary or nominee arrangement, including the power to direct, withhold, consent to or veto the exercise of any power related to the legal structure or fiduciary or nominee arrangement;

(iii) satisfactory identification evidence of all persons providing funds or assets to the structure;

(iv) the applicable documents, identifying the known beneficiaries of the trust;

(v) the applicable documents, identifying beneficiaries of a fiduciary or nominee structure;

(vi) the applicable documents, appointing and identifying any signatory powers in relation to the legal structure or fiduciary or nominee arrangement; and

(vii) satisfactory evidence of the identity of persons authorised to undertake transactions;

(e) a foundation —

(i) the foundation Charter;

(ii) the foundation's certificate of registration issued by the Registrar General, or the foreign equivalent;

(iii) the source of funds, and where a person other than the founder provides funds for the foundation, verification of the identity of the third party providing the funds or for whom the founder may be acting;

(iv) identification evidence of each founder, officer, and council member of the foundation as may be signatories for the accounts of the foundation;

(v) identification evidence of beneficiaries that hold a vested interest in the foundation; and

(vi) satisfactory evidence of the identity of the persons authorised to undertake transactions;

(f) a non-profit association or charity —

(i) identification evidence of at least two signatories, and any person authorised to give instructions on behalf of the entity;

(ii) the nature of the proposed association's or charity's purpose and operations;

(iii) the source of funds; and

(iv) satisfactory evidence of the identity of the persons authorised to undertake transactions;

(g) powers of attorney —

(i) identification of each donee;

(ii) identification evidence of the donor;

(iii) proof of any third party mandates; and

(iv) satisfactory evidence of the identity of the persons authorised to undertake transactions.

(2) A registrant shall, in the case of services being provided to the estate of a deceased person, obtain identification evidence of each personal representative of the estate.

(3) A registrant shall review its records periodically to ensure that the identification and other information kept by it is current and reflects the existing facts related to a customer, and in any cases when there have been changes to —

(a) persons authorised to undertake transactions;

(b) board resolutions or mandates authorising the opening of an account and authorising any person to undertake transactions;

(c) partners, controllers, trustees, fiduciaries or nominees; and

(d) the corporate structure of a customer.

(4) Where there has been a change to any of the items specified under paragraph (3), the registrant shall undertake the verification process in compliance with this rule.

(5) For the purpose of the verification process, a registrant shall exercise additional care in relation to the provision of trading services with respect to digital assets with anonymity enhancing features or that obscure a user’s identity or other transactional information.

(6) Where a registrant offers the service specified under paragraph (5), the registrant shall independently verify the identity of the proposed facility

holder and any beneficial owner through reliable and independent source documents, data, or information.

(7) A registrant shall maintain, in any case, adequate documentation to evidence the implementation of due diligence measures and shall ensure that the verification of identification procedures implemented are appropriate to the nature and structure of the proposed customer being verified.

(8) A registrant shall, as part of due diligence measures, implement procedures for the periodic re-verification of customers, which at the minimum, shall require re-verification to occur where —

(a) during the course of the business relationship, the registrant has reason to doubt the identity of the customer;

(b) there is a material change in the way transactions are undertaken; or

(c) there is a reasonable suspicion that any transaction carried out by the customer might have breached the law concerning identified risks.

18. Politically exposed persons.

(1) A registrant shall, in addition to applying enhanced due diligence measures, develop clear procedures and controls for the identification and verification of a politically exposed person when —

(a) establishing a business relationship with that politically exposed person, or a legal person in which any politically exposed person —

(i) is a director, officer, founder or council member;

(ii) is a partner or trustee;

(iii) is a signatory or person authorised to undertake transactions;

(iv) has a beneficial interest of ten per cent or more in the legal person;

(v) has principal control over the legal person's assets;

(vi) exercises control over the management of the legal person; or

(b) the registrant is continuing a business relationship with a customer who has become a politically exposed person, after the establishment of the business relationship.

(2) In relation to a politically exposed person referred to under subparagraph (a)(ii) of the definition of politically exposed person under paragraph (5), whether as customer or beneficial owner, a registrant shall —

(a) obtain the approval of senior management before establishing the business relationship or, where the customer or beneficial owner

becomes such a person after the establishment of the business relationship, before continuing the business relationship;

(b) take reasonable measures to establish the source of wealth and the source of funds of the customer or beneficial owner; and

(c) conduct enhanced ongoing monitoring of the business relationship.

(3) In relation to a politically exposed person referred to under subparagraph (a)(i) or (a)(iii) of the definition of politically exposed person under paragraph (5), a registrant shall take reasonable measures to determine whether a customer or beneficial owner is such a person and, where the business relationship with such a person presents a higher risk, shall apply the measures set out under paragraph (2).

(4) Paragraphs (2) and (3) apply, with the necessary changes, to the individuals and entities referred to under paragraphs (b), (c) and (d) of the definition of politically exposed person under paragraph (5).

(5) For the purposes of this rule —

"international organisation" means an entity established by a formal political agreement equivalent in status to an international treaty, made between, and recognised by law, in member countries, and which is not treated as a resident institutional unit of the country in which it is located;

"politically exposed person" means —

(a) an individual who is or has been entrusted with —

(i) a prominent public function within The Bahamas, inclusive of a head of state or government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or an important political party official;

(ii) a prominent public function by a foreign jurisdiction, inclusive of, a head of state or government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or senior political party official; or

(iii) a prominent function within an international organisation, including directors, deputy directors, members of the board, members of senior management, or individuals who have been entrusted with equivalent functions;

(b) an individual who is a family member of an individual referred to under paragraph (a), being an individual related to

that individual directly or through marriage or a similar form of partnership, including a spouse or partner, parent, child or sibling;

(c) an individual who is closely associated to a politically exposed person either socially, or professionally and includes a person who can conduct substantial domestic or international financial transactions on behalf of the politically exposed person;

(d) any corporation, business or other entity formed by or for the benefit of a head of state, head of government or individuals referred to under paragraph (a).

19. Reliance on third party verification procedures.

(1) A registrant may rely on the customer due diligence procedures implemented by another virtual asset service provider or financial institution, provided that the virtual asset service provider or financial institution is a regulated entity subject to anti-money laundering, countering the financing of terrorism and countering the financing of proliferation obligations and is an entity located in a country which is not the subject of any list issued by an international organisation relative to the issues of activities associated with identified risks, and is able to —

(a) provide written confirmation that it has verified the identity of the relevant customer; and

(b) confirm the existence of the account or facility provided to the customer by the virtual asset service provider or financial institution.

(2) Notwithstanding paragraph (1), a registrant shall only rely on the due diligence measures implemented by another virtual asset service provider or financial institution with respect to those categories of transactions, services, or products which that other virtual asset service provider or financial institution provides to the customer, and in any other circumstance, must undertake its own verification procedures.

20. Eligible introducer.

(1) A registrant's duty to verify the identity of prospective customers shall apply to any customer introduced by another virtual asset service provider or financial institution, except where a virtual asset service provider or financial institution is an eligible introducer.

(2) Where a registrant relies on the verification procedures of an eligible introducer, the registrant shall obtain from that introducer —

(a) written confirmation that the eligible introducer has verified the customer's identity in accordance with the national laws of the eligible introducer;

(b) certification from the eligible introducer that any photocopies provided to the registrant are identical to the original document; and

(c) clear and legible copies of documentation, including where appropriate, certified translations, within thirty days of receipt of the written confirmation referred to under subparagraph (a).

(3) For the purposes of this paragraph, an eligible introducer shall be —

(a) in relation to a domestic financial institution —

(i) a person registered under Part VII of the Securities Industry Act;

(ii) an investment fund administrator licensed under section 34 of the Investment Funds Act;

(iii) a bank or trust company licensed by the Central Bank of The Bahamas under the Banks and Trust Companies Regulation Act;

(iv) a digital asset business registered under the Act; or

(b) in relation to a foreign virtual asset service provider or financial institution, a service provider or institution —

(i) exercising functions similar to a domestic digital asset business or financial institution to which subparagraph (a)(i) through (iv) applies;

(ii) registered or functioning pursuant to Part VII of the Securities Industry Act;

(iii) located in a country which is not the subject of any list issued by an international organisation relative to the issues of activities associated with identified risks; and

(iv) having no obstacles, administrative or otherwise, that would prevent the registrant from accessing the original documentation.

21. Suspension or termination of activity or business.

A registrant shall —

(a) suspend activity on the account of a prospective customer, if reasonable efforts have been made to directly verify the prospective customer's identity without success;

(b) terminate the business relationship with a prospective customer where it is unable to obtain the relevant information and

documentation from the eligible introducer within thirty days of receiving the eligible introducer's confirmation;

(c) refuse, suspend, or terminate any transaction involving an unhosted wallet where —

(i) the registrant's customer is unable to or has failed to obtain or provide the required details and information regarding the counterparty institution and unhosted wallet related to the relevant transaction;

(ii) the unhosted wallet address is linked to illicit activity, sanctions targets, or unauthorized mixing services; or

(iii) the risks associated with the transaction cannot be effectively mitigated.

22. Simplified verification for specified customers.

(1) A registrant may treat a prospective customer as presenting a lower risk for the purposes of rule 13, and may apply simplified due diligence measures in accordance with that rule, where the prospective customer is —

(a) a digital asset business or financial institution licensed or registered by the Central Bank of The Bahamas, the Securities Commission of The Bahamas, the Insurance Commission of The Bahamas, the Compliance Commission or the Gaming Board for The Bahamas;

(b) a virtual asset service provider or financial institution which —

(i) is subject to obligations to combat money laundering, the financing of terrorism and the financing of proliferation consistent with the recommendations of the Financial Action Task Force;

(ii) is supervised for compliance with the obligations referred to under subparagraph (i); and

(iii) has adequate procedures in place for compliance with customer due diligence and record keeping requirements;

(c) a central or local government agency or statutory body; or

(d) a publicly traded company listed on a marketplace registered by the Commission or an exchange specified under the Schedule to the Financial Transactions Reporting Regulations, which is subject to disclosure requirements ensuring adequate transparency of beneficial ownership.

(2) Nothing in paragraph (1) exempts a registrant from the requirement to identify a prospective customer, and rule 15(1), (4) and (5) shall apply to the application of simplified due diligence measures under this rule.

23. Ongoing monitoring.

(1) A registrant shall, after the verification procedures have been concluded and a business relationship has been established —

(a) monitor the conduct of the business relationship periodically; and

(b) ensure, on an ongoing basis, that the business relationship is consistent with the risk profile and nature of the business stated when the relationship was established.

(2) Ongoing monitoring of business relationships includes, without limitation —

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the registrant's knowledge of the customer, their business and risk profile;

(b) ensuring that the source documents, data or other information obtained for the purposes of applying due diligence are kept up to date;

(c) analysing blockchain and similar transactions in line with a risk-based approach including, without limitation, taking into account the nature of the registrant's business and whether it is appropriate to use such analysis for transactions;

(d) where large volumes of transactions occur on a regular basis, using automated systems to monitor transactions provided that flagged transactions are subject to human expert analysis to determine whether such transactions are suspicious.

PART V — TRANSFERS OF DIGITAL ASSETS

24. Transfers of digital assets.

(1) In this Part —

"required originator information" and **"required beneficiary information"** mean the originator information and the beneficiary information required to accompany a transfer pursuant to regulations 4 and 7 of the Financial Transactions Reporting (Wire

Transfers) Regulations, as those Regulations apply to transfers of digital assets;

"immediately" means before or at the time the transfer of digital assets is conducted; and

"securely" means in a manner which protects the information from unauthorised disclosure and which preserves the integrity and availability of the information.

(2) A registrant which acts as an ordering institution shall —

(a) obtain and hold required and accurate originator information and required beneficiary information in respect of each transfer of digital assets;

(b) submit the information referred to under subparagraph (a) to the beneficiary institution or, where applicable, to an intermediary institution, immediately and securely; and

(c) not execute the transfer where it is unable to comply with subparagraphs (a) and (b).

(3) A registrant which acts as an intermediary institution shall —

(a) ensure that all originator and beneficiary information received with a transfer of digital assets is retained with, and accompanies, the transfer;

(b) take reasonable measures, consistent with straight through processing, to identify transfers which lack required originator information or required beneficiary information; and

(c) adopt risk-based policies and procedures for determining when to execute, reject or suspend a transfer lacking required information, and the appropriate follow up action.

(4) A registrant which acts as a beneficiary institution shall —

(a) obtain and hold required originator information and required and accurate beneficiary information in respect of each transfer of digital assets;

(b) verify the identity of the beneficiary in accordance with these Rules, where the identity of the beneficiary has not previously been verified;

(c) take reasonable measures to identify transfers which lack required originator information or required beneficiary information; and

(d) adopt risk-based policies and procedures for determining when to execute, reject or suspend a transfer lacking required information, and the appropriate follow up action.

(5) A registrant shall make the information obtained and held under this rule available promptly upon request to the Commission, the Financial Intelligence Unit and any other authority lawfully entitled to request it, and to law enforcement authorities pursuant to lawful process.

(6) This rule is in addition to, and does not derogate from, the obligations of a registrant under the Financial Transactions Reporting (Wire Transfers) Regulations.

25. Counterparty institutions.

(1) Before submitting required originator information or required beneficiary information to a counterparty institution, a registrant shall take reasonable measures —

(a) to identify the counterparty institution; and

(b) to determine whether the counterparty institution is subject to obligations to combat money laundering, the financing of terrorism and the financing of proliferation, and can reasonably be expected to protect the confidentiality of the information submitted and to comply with obligations corresponding to those of this Part.

(2) The measures taken under paragraph (1) shall be applied on a risk basis and may rely on an assessment of a counterparty institution previously conducted by the registrant, provided that the assessment is reviewed and kept up to date, and the outcome of those measures shall inform the registrant's determination whether to execute, reject or suspend a transfer of digital assets and the appropriate follow up action.

26. Transfers involving unhosted wallets.

(1) Where a transfer of digital assets is made to, or received from, an unhosted wallet, the registrant shall obtain the required originator information and the required beneficiary information in respect of the transfer from its customer.

(2) A registrant shall assess transfers to or from unhosted wallets in accordance with its risk rating framework, having regard to rule 3(2)(k), and where a higher risk is presented shall apply risk mitigation measures commensurate with that risk, which may include the measures described under rule 14(4) and limits on, or enhanced monitoring of, such transfers.

PART VI – TARGETED FINANCIAL SANCTIONS

27. Targeted financial sanctions.

(1) A registrant shall establish and maintain policies, procedures, systems and controls to ensure its compliance with targeted financial sanctions, which shall include the implementation of sanctions against a designated person or entity, pursuant to section 3A of the International Obligations (Economic and Ancillary Measures) Act and section 44 of the Anti-Terrorism Act to —

(a) freeze, without delay or notice to the designated person or entity, funds or other assets —

(i) of designated persons and entities that are owned or controlled, by designated persons or entities;

(ii) derived or generated from funds or other assets owned or controlled by designated persons or entities;

(iii) of persons and entities acting on behalf of or at the direction of a designated person or entity;

(b) inform the Attorney-General and the Financial Intelligence Unit that the registrant holds funds and other assets owned or controlled by a designated person or entity; and

(c) inform the designated person or entity that the funds held by the registrant have been frozen.

(2) A registrant shall cooperate with any legal action for the forfeiture or confiscation of any money, asset or property frozen in accordance with the implementation of targeted financial sanctions.

(3) For the purposes of paragraph (1) —

(a) funds or other assets owned or controlled by a designated entity include money, property, tangible or intangible assets or digital assets;

(b) owned or controlled includes whole or joint ownership or direct or indirect control.

PART VII - RECORD KEEPING

28. Maintenance of records.

(1) A registrant shall, in compliance with relevant laws, prepare and maintain records of its business relationships and transactions that enable —

(a) competent third parties to assess the registrant's compliance with anti-money laundering, countering the financing of terrorism and countering the financing of proliferation policies and procedures;

(b) transactions effected through the registrant to be reconstructed;

(c) the registrant to satisfy court orders or enquiries from the Commission or appropriate authorities; and

(d) the identification of the customer.

(2) A registrant shall keep records required to be maintained by these Rules, for a period of seven years from the date that the customer ceases to be a facility holder.

(3) For the purpose of paragraph (2), a person ceases to be a facility holder from the date of —

(a) the carrying out of a one-off transaction or the last transaction in a series of transactions;

(b) the closing of the account(s) or the ending otherwise of the business relationship; or

(c) the commencement of proceedings to recover debts payable on insolvency.

(4) The seven-year period referred to under paragraph (2) commences on the date of the completion of the last transaction where formalities to end a business relationship have not been undertaken but a period of seven years has elapsed since the date of the last transaction.

(5) Where the registrant is a company that is being liquidated, the liquidator shall retain the relevant records of the regulated person for the balance of the prescribed period remaining at the date of dissolution.

(6) The registrant may maintain records in the form of original documents or other electronic media provided —

(a) there are appropriate internal controls in place to guard against the risk of loss, damage, destruction or falsification

(b) such method provides a means to immediately provide to the Commission, upon request, legible, true and complete copies of those records; and

(c) the registrant has suitable back-up and disaster recovery programs.

29. Transaction records.

A registrant shall maintain transaction records containing —

(a) a description of the nature of the transaction;

(b) details of the transaction, including the amount of the transaction and the denomination of the currency;

(c) the date on which the transaction was conducted;

(d) the identification verification details of the parties to the transaction;

(e) the public keys (or equivalent identifiers) of relevant parties;

(f) where applicable, information on the facility through which the transaction was conducted and any other facility directly involved in the transaction; and

(g) the files, business correspondence, and records connected to the facility.

30. Other records.

A registrant shall maintain records of —

(a) suspicions raised internally by the Money Laundering Reporting Officer, but not disclosed to the relevant authorities;

(b) suspicions which the Financial Intelligence Unit, the Commissioner of Police, or the relevant supervisory authority have advised are of no interest; and

(c) findings of inquiries conducted by the registrant into unusual activity.

PART VIII - MISCELLANEOUS

31. Education and training.

(1) A registrant shall take appropriate measures to ensure that each employee is aware of —

(a) the policies and procedures put in place to detect and prevent money laundering, to counter the financing of terrorism and to counter the financing of proliferation, including those for the identification, record keeping, detection of unusual and suspicious transactions and internal reporting; and

(b) the anti-money laundering, countering the financing of terrorism and countering the financing of proliferation legislative framework.

(2) A registrant shall ensure that —

(a) the relevant staff members and key personnel are trained on an ongoing basis to —

(i) identify, prevent, detect and disclose financial crime risks;

(ii) recognise and handle suspicious transactions;

(b) its key personnel possess the adequate knowledge, skills, experience and capability to understand the registrants' business and customer needs;

(c) key personnel and staff are aware of their obligations to comply with policies and procedures.

32. Revocation of S.I. No. 32 of 2022.

The Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation) Rules, 2022 are revoked.

Made this 27th day of October, 2026.

Signed
PETER T. CAREY
DEPUTY CHAIRMAN
SECURITIES COMMISSION OF THE BAHAMAS