SECURITIES COMMISSION OF THE BAHAMAS

# PUBLIC CONSULTATION

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

CONSULTATION PERIOD:
MONDAY 10 AUGUST 2026 - MONDAY 31 AUGUST 2026

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

The Securities Commission of The Bahamas ("the Commission"), in its capacity as the regulator of digital assets businesses and digital assets exchanges, pursuant to the Digital Assets and Registered Exchanges Act 2024, issues this draft Rules for public consultation. The draft Rules can be found on the Commission's website at: scb.gov.bs/legislative-framework/consultation-documents/.

**Summary/Purpose**

The Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation) (Amendment) Rules, 2026 were developed to amend the Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation) Rules, 2022. The main objective of the Rules is to ensure consistency across the various Rules issued by the Commission and incorporate amendments made to the Financial Transactions Reporting Act, 2018.

**Scope**

These Rules would apply to all regulated persons under the Digital Assets and Registered Exchanges Act, 2024.

**Consultation period**

Commences: Monday 10 August 2026
Ends: Monday 31 August 2026

**Reply to:**

Please submit any comments to **DAREconsultation@scb.gov.bs.**

**Or alternatively, to:**

Executive Director
Securities Commission of The Bahamas
Poinciana House North Building
2nd Floor, 31A East Bay Street
P.O. Box N-8347
Nassau, The Bahamas
Tel: (242) 397-4100
Email: info@scb.gov.bs

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

**Arrangement of Sections**

# DIGITAL ASSETS AND REGISTERED EXCHANGES ACT
# (CHAPTER 369)

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

The Minister, in exercise of the powers conferred by section 81 of Digital Assets and Registered Exchanges Act, 2024 (*No. 40 of 2024*), makes the following Rules —

## 1. Citation.

These Rules, which amend the Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering the Financing of Terrorism and Countering the Financing of Proliferation) Rules, 2022, may be cited as the Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering the Financing of Terrorism and Countering the Financing of Proliferation) (Amendment) Rules, 2026 —

## 2. Insertion of new 3A into the principal Rules.

The principal Rules is amended by the insertion, immediately after rule 8, of the following new rule –

**“3A. Risk-based Monitoring**

A registrant shall maintain continuous, risk-based monitoring of all virtual asset transactions executed or facilitated through their platform, by a counterparty that is a VASP or an unhosted wallet.”

## 3. Amendment of rule 4 of the principal Rules.

Rule 4 of the principal Rules is amended —

(a) in paragraph (1) —

(i) in the chapeau, by the deletion of the words “identified risks associated with money laundering, the financing of terrorism and the financing of proliferation” and the substitution of the words, “activity related to identified risks”; and

(j) in sub-paragraph (c), by the deletion of the words “money laundering and the financing of terrorism and the financing of proliferation activities: and the substitution of the words “identified risks”; and

(b) in paragraph (3), by the deletion of the words “money laundering and the financing of terrorism and the financing of proliferation”.

(c) by the renumbering of paragraphs (2) and (3) as paragraphs (3) and (4).

(d) by the insertion immediately after paragraph (1), of the new paragraph (2) as follows –

"(2) a registrant shall establish and maintain procedures to enable the registrant to distinguish between transactions conducted with another registrant or regulated digital asset business and transactions conducted with an unhosted wallet."

(e) by the insertion immediately after paragraph (4), of the new paragraphs (5) and (6) as follows –

"(5) A registrant shall employ automated blockchain analytics software to assess the risk score of all unhosted wallet addresses involved in transfers.

(6) An unhosted wallet address shall be flagged as high-risk if on-chain analytics indicate prior interaction with:

(i) Decentralized mixers or anonymizing tools (e.g., CoinJoin, privacy pools);

(ii) Darknet marketplaces, ransomware addresses, or illicit platforms;

(iii) Unregistered or non-compliant high-risk exchanges."

## 4. Insertion of new rules 4A, 4B, 4C, 4D, 4E and 4F into the principal Rules.

The principal Rules is amended by the insertion, immediately after rule 4, of the following new rules —

### "4A. Obligation to Maintain Continuous Transaction Monitoring Systems.

(1) A registrant shall establish, implement, and maintain an automated, risk-based transaction monitoring system capable of screening and analyzing all virtual asset transfers/transactions executed, facilitated, or received by the registrant on a continuous and real-time basis.

(2) The transaction monitoring system shall operate across all underlying distributed ledgers, blockchains, sidechains, or cross-chain protocols supported by the registrant.

(3) A registrant shall correlate on-chain transaction metadata with off-chain customer profile data, including:

(a) customer risk rating and source of funds declarations;

(b) historical transaction volume, frequency, and typical counterparty profiles;

(c) information collected pursuant to Customer Due Diligence and Travel Rule compliance obligations.

### 4B. Mandatory Red Flag Indicators and Alert Configuration.

(1) A registrant's transaction monitoring framework must be configured to generate real-time alerts upon detecting transaction patterns or indicators consistent with high-risk or suspicious activity, including but not limited to:

(a) transfers/transactions originating from, or directed to, decentralized mixers, privacy pools, coinjoin software, or privacy-focused protocols;

(b) rapid sequential transactions across multiple assets or blockchains without clear economic or commercial rationale;

(c) multiple transfers executed immediately below regulatory reporting or Travel Rule thresholds within a defined time window;

(d) sudden high-value or high-velocity transfer activity involving wallet addresses that have remained inactive for extended periods; and

(e) rapid deposit and immediate full withdrawal of virtual assets with minimal holding duration.

## 4C. Counterparty Risk Scoring and On-Chain Intelligence.

(1) Every registrant shall utilize verified blockchain analytics tools to assess and assign a risk score to all counterparty wallet addresses prior to finalizing a transaction or crediting customer funds.

(2) An on-chain address shall be designated as high-risk if blockchain intelligence demonstrates direct or indirect exposure (within a risk-appropriate hop limit) to:

(a) designated individuals or entities on official targeted financial sanctions lists;

(b) darknet marketplaces, ransomware actors, or illicit exploitation protocols;

(c) non-compliant, unregistered, or high-risk exchanges operating without adequate anti-money laundering, countering the financing of terrorism and countering the financing of proliferation supervision.

## 4D. Suspicious Activity Reporting and Transaction Holds.

(1) Where transaction monitoring generates an alert indicating potential money laundering, terrorist financing, or proliferation financing, the registrant shall immediately place a temporary operational hold on the affected transfer pending an internal compliance investigation.

(2) If internal review confirms reasonable grounds to suspect that funds are derived from criminal activity or linked to terrorist financing, the registrant shall comply with section 5(1)(c).

## 4E. Travel Rule Data Discrepancy Monitoring.

(1) A registrant’s transaction monitoring systems shall cross-examine information received via Travel Rule protocols against on-chain transaction logs.

(2) The registrant shall flag for review any transaction where:

(a) the originator or beneficiary name/identifier transmitted via the Travel Rule message conflicts with the verified attribution data of the on-chain address; or

(b) required Travel Rule metadata is missing, incomplete, or altered during transit.

**4F. Record Retention and Auditability.**

A registrant shall maintain comprehensive, tamper-evident electronic records of all transaction monitoring logs, generated alerts, risk-scoring outputs, and compliance investigation files."

## 5. Amendment of rule 5 of the principal Rules.

Rule 5 of the principal Rules is amended in sub-paragraph (1)(c), by the insertion immediately after the word "reports" of "promptly", and by the deletion of the words "money laundering, and the financing of terrorism and the financing of proliferation" and the substitution of the words, "activity related to identified risks".

## 6. Insertion of new rules 6A, 6B, 6C, 6D, 6E and 6F into the principal Rules.

The principal Rules is amended by the insertion, immediately after rule 6, of the following new rules —

**"6A. 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.

**6B. Mandatory Initial and Ongoing Due Diligence.**

(1) Prior to entering into any arrangements with a third-party technology provider for critical or regulated functions[1] a registrant shall conduct and document a comprehensive due diligence assessment

(2) The due diligence assessment shall evaluate, at a minimum:

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

[1] Guidance to provide critical or regulated functions include travel rule messaging protocols, blockchain analytics (KYT), customer due diligence (CDD/KYC), or wallet custody infrastructure

(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.

(3) 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.

## 6C. Mandatory Contractual Provisions.

Every outsourcing or third-party technology agreement involving a regulated function shall be governed by a written, legally binding contract that includes the following explicit provisions:

(a) A registrant shall have immediate and unrestricted rights to access and retrieve all customer due diligence records, transaction logs, analytics outputs, and audit trails held by the vendor;

(b) a registrant, its independent auditors, and the supervisory authority shall have the contractual right to inspect, audit, and test the vendor's software, hardware, operational controls, and data centers upon reasonable notice;

(c) strict obligations enforcing compliance with applicable data privacy, metadata protection, and encryption requirements to prevent unauthorized disclosure or misuse of customer data;

(d) a requirement that the vendor obtain prior written consent from the registrant before sub-contracting or sub-outsourcing any core component of the service to a fourth-party provider;

(e) An obligation on the vendor to notify the registrant within 24 hours of detecting any cybersecurity breach, system failure, or regulatory non-compliance affecting the outsourced functions.

## 6D. Immediate Information Availability.

Where a registrant relies on a third party to execute customer identification, verification, or Travel Rule data collection:

(a) The registrant shall immediately obtain from the third party the necessary customer due diligence and transaction metadata; and

(b) The registrant shall satisfy itself that copies of identification data and other relevant documents will be made available by the third party without delay upon request.

(c) Copies of identification data and underlying verification documents must be accessible from the third party without delay upon request by the Commission or the registrant.

### 6E. Prior Regulatory Notification of Material Outsourcing.

(1) A registrant shall submit formal written notification to the supervisory authority at least 30 to 60 days prior to entering into, or materially altering, any outsourcing arrangement involving a critical technical or compliance function.

(2) The notification shall include a copy of the risk assessment, draft contract terms, business continuity plans, and designated compliance contacts at the third-party provider.

### 6F. Business Continuity, Exit Strategies, and Vendor Lock-In

(1) A registrant shall maintain an active, tested business continuity plan and disaster recovery protocol capable of sustaining uninterrupted compliance monitoring during vendor system outages or network disruptions.

(2) A registrant shall establish a documented, viable exit strategy for every material technology arrangement, detailing data migration protocols and contingency plans in the event of vendor insolvency, contract termination, or regulatory disqualification."

## 7. Amendment of rule 7 of the principal Rules.

Rule 7 of the principal Rules is amended in subparagraph (1)(c) is repealed and replaced as follows –

"(c) for overseeing and managing the making of suspicious transaction reports promptly regarding a transaction or any proposed transaction relating to the proceeds of criminal conduct or which constitutes an offence under the Proceeds of Crime Act, 2018 *(No. 4 of 2018),* or which is an identified risk."

## 8. Insertion of rule 7A into the principal Rules.

The principal Rules is amended by the insertion, immediately after rule 7, of the new rule 7A as follows –

### "7A. Implementation of Targeted Financial Sanctions.

(1) A registrant shall comply with the Anti-Terrorism Act, 2018, including the procedures for implementing the United Nations Security Council Resolutions.

(2) A registrant shall without delay and without prior notice:

(a) freeze all of the funds it holds in the name of a designated person or entity;

(b) inform the Attorney General and Financial Intelligence Unit that it holds the funds of a designated person or entity and provide details;

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

(3) The freezing shall extend to:

(a) all funds that are owned or controlled by the designated person or entity;

(b) funds that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities;

(c) funds derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities; and

(d) funds of persons and entities acting on behalf of, or at the direction of designated persons or entities.

(4) A registrant shall not make any funds available, directly or indirectly, to or for the benefit of a designated person or entity."

## 9. Amendment of rule 8 of the principal Rules.

Rule 8 of the principal Rules is amended in paragraph (3), by the insertion immediately after the word "date" of "on the basis of materiality and risk, at appropriate times, taking into account the adequacy of data obtained when previous customer due diligence measures were undertaken."

## 10. Revocation and replacement of rule 9 of the principal Rules.

Rule 9 of the principal Rules is repealed and replaced as follows –

"**9. Simplified due diligence.**

(1) Where a registrant determines, on the basis of its risk assessment that a client presents a lower risk, the registrant may apply simplified due diligence measures to verify the identity of that client, provided that such measures are not applied where there is a suspicion of identified risks.

(2) Where the registrant intends to utilise a simplified due diligence procedure—

(a) the registrant shall submit to the Commission a written outline of the registrant's risk rating procedure and proposed simplified due diligence process;

(b) the Commission shall review the proposed simplified due diligence process and, where satisfied that the process is appropriate and consistent with these Rules, approve the registrant to proceed with the verification of the client utilising due diligence measures appropriate to the client's level of risk.

## 11. Amendment of rule 10 of the principal Rules.

Rule 10 of the principal Rules is amended in paragraph (1), by the deletion of the words "money laundering, or the financing of terrorism or the financing of proliferation" and the substitution of the words, "activity related to identified risks".

(a) in paragraph (2), by the deletion of the words "money laundering, or the financing of terrorism or the financing of proliferation activities: and the substitution of the words "activity related to identified risks"; and

(b) in paragraph (3), by the deletion of the words "money laundering, or the financing of terrorism or the financing of proliferation activities: and the substitution of the words "activity related to identified risks".

## 12. Amendment of rule 11 of the principal Rules.

Rule 11 of the principal Rules is amended

(a) by the renumbering of paragraphs (2) – (6) as paragraphs (3) – (7).

(b) by the insertion immediately after paragraph (1), of the new paragraph (2) as follows –

"Subject to paragraph (1), where any virtual asset transaction involves an unhosted wallet, a registrant shall:

(a) obtain from its customer the name and identifying information of the counterparty associated with the unhosted wallet; and

(b) in relation to the unhosted wallet address provided by its customer, conduct:

(i) a real-time or post-transaction risk assessment; and

(ii) screen the unhosted wallet address and counterparty details against global sanctions lists."

(c) in paragraph (6), by the deletion of the words "money laundering, or the financing of terrorism or the financing of proliferation activities: and the substitution of the words "activity related to identified risks".

## 13. Amendment of rule 12 of the principal Rules.

Rule 12 of the principal Rules is amended in sub-paragraph (8)(c) by the deletion of the words "money laundering, the financing of terrorism or the financing of proliferation" and the substitution of the words, "identified risks".

## 14. Amendment of rule 14 of the principal Rules.

Rule 14 of the principal Rules is amended in paragraph (1) by the deletion of the words "of money laundering, or the financing of terrorism or the financing of proliferation activities," and the substitution of the words, "activities associated with identified risks,".

## 15. Amendment of rule 15 of the principal Rules.

Rule 15 of the principal Rules is amended in paragraph (3)(b)(iii) by the deletion of the words "of money laundering or the financing of terrorism or the financing of proliferation" and the substitution of the words, "activities associated with identified risks".

## 16. Amendment of rule 16 of the principal Rules.

Rule 16 of the principal Rules is amended by the insertion immediately after paragraph (b) of the new paragraph (c) as follows-

“(c) A registrant shall 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 and unhosted wallet related to the relevant transaction(s);

(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.”