SECURITIES COMMISSION OF THE BAHAMAS

PUBLIC CONSULTATION

WALLET INFORMATION COLLECTION AND SCREENING POLICY

CONSULTATION PERIOD:
THURSDAY 6 AUGUST 2026 - FRIDAY 21 AUGUST 2026

DRAFT WALLET INFORMATION COLLECTION AND SCREENING POLICY

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, issues this draft policy for public consultation.

Summary/Purpose

This policy aims to establish the obligation of licensees and registrants under the Digital Assets and Registered Exchanges Act ("the DARE Act"), and of applicants for registration, to provide wallet information to the Securities Commission of The Bahamas and states the purposes for which the Commission collects, holds and screens that information.

Scope

The finalized policy will apply to every person licensed or registered under the DARE Act, and to every applicant for such licence or registration, in each case to the extent of the digital asset business conducted or proposed.

Consultation period

Commences:	Thursday 6 August 2026
Ends:	Friday 21 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
Fax: (242) 356-7300
Email: info@scb.gov.bs

Part I — Introduction and Application

1.1 This Policy establishes the obligation of licensees and registrants under the Digital Assets and Registered Exchanges Act (“the DARE Act”), and of applicants for registration, to provide wallet information to the Securities Commission of The Bahamas (“the Commission”), and states the purposes for which the Commission collects, holds and screens that information.

1.2 This Policy is made in furtherance of the Commission's supervisory functions and information-gathering powers under section 56 of the DARE Act and section 54 of the Securities Industry Act.

1.3 This Policy applies to every person licensed or registered under the DARE Act, and to every applicant for such licence or registration, in each case to the extent of the digital asset business conducted or proposed.

Part II — Obligation to Provide Wallet Information

2.1 Wallet information in accordance with the Schedule shall be provided to the Commission at three points:

(a) Authorisation — as part of the application for licensing or registration, in respect of the wallets the applicant operates or proposes to operate;

(b) Material change — within ten (10) business days of establishing, retiring or materially altering any wallet within a category in the Schedule to this Policy, including migration of client assets between wallets; and

(c) Annual attestation — annually, on the date and in the form specified by the Commission, attesting to the completeness and currency of the licensee's or registrant's entries in the Commission's records.

2.2 Information provided under this Policy shall be accurate and complete. Provision of information under this Policy does not discharge any other reporting or notification obligation under the DARE Act or any other law.

Part III — Purposes and Use

3.1 The Commission collects wallet information solely for the following purposes:

(a) assessment of applications for licensing or registration, including source-of-funds analysis;

(b) ongoing risk-based supervision of the licensed and registered population, including periodic and event-driven screening using blockchain analytics;

(c) examination of licensees and registrants; and

(d) the discharge of the Commission's functions under the DARE Act, the Securities Industry Act, the Financial Transactions Reporting Act and the Anti-Terrorism Act, including enforcement thereof.

3.2 Wallet information shall not be used for any purpose other than those stated in paragraph 3.1, and shall be held as confidential regulatory information subject to the Commission's confidentiality obligations. Disclosure outside the Commission occurs only through lawful gateways, including with the express consent of the person to whom the information relates, to the Financial Intelligence Unit and domestic law enforcement, and to foreign regulatory counterparts under the Commission's cooperation arrangements.

3.3 Screening under this Policy is a supervisory activity. A screening result is not, of itself, a finding against a licensee, registrant or applicant; the Commission will put material adverse indications to the person concerned and provide them with an opportunity to respond before drawing supervisory conclusions from them.

Part IV — Compliance

4.1 Failure to provide wallet information as required by this Policy, the provision of inaccurate or incomplete information, or failure to attest annually, is a supervisory matter and may constitute a contravention of the licensee's or registrant's obligations under the DARE Act, rendering the licensee or registrant liable to the supervisory and enforcement consequences provided thereunder.

4.2 An applicant's failure to provide the particulars required by the Schedule to this Policy, as part of the information required for an application, may result in the application being treated as incomplete.

Part V — Commencement

5.1 This Policy shall be issued, following approval by the Executive Director and the Board of the Commission and industry consultation, and shall take effect on the date stated at issue (“the effective date”). The first annual attestation date shall be set not earlier than six (6) months after the effective date.

5.2 Wallet information lawfully held by the Commission at the effective date, including information provided at authorisation, forms the opening record for each licensee and registrant.

Schedule — Wallet Information Particulars

Item	Particulars to be provided
1. Wallet addresses	Each operational wallet, by address and network/chain, in each applicable category: (a) client-asset custody wallets (hot and cold); (b) treasury and proprietary wallets; (c) fee-collection wallets; (d) omnibus or pooled wallets; (e) settlement wallets used with counterparties.
2. Proof of control	For each wallet in categories (a), (b) and (d): evidence of control by cryptographically signed message in the form specified by the Commission, or by micro-transaction as the Commission directs.
3. Source of funds (applicants)	For capital and principal treasury balances: originating wallet addresses or exchange accounts; dates and amounts of funding transactions; and, for fiat-originated funds, the on-ramp or institution used.
4. Counterparty relationships	Principal exchange, liquidity, custody and settlement relationships, and, where used, the deposit addresses employed with each counterparty.
5. Entity identifiers	The names, trading names and group entities under which the licensee or registrant operates or is known on-chain or on analytics platforms.
6. Principals' wallets	Not required as a standing obligation. The Commission may require a beneficial owner, director or senior officer to declare wallets used in connection with the business where the Commission considers it necessary to its assessment.