SECURITIES COMMISSION OF THE BAHAMAS

GUIDANCE NOTE

TRAVEL RULE COMPLIANCE FOR DIGITAL ASSET BUSINESSES

PUBLISHED DATE: 12 AUGUST 2026

GUIDANCE NOTE — TRAVEL RULE COMPLIANCE FOR DIGITAL ASSET BUSINESSES

For Digital Asset Businesses Registered under the Digital Assets and Registered Exchanges Act, 2024

TABLE OF CONTENTS

Part I — Status, Purpose and Application

1.1 This Guidance Note explains how the Securities Commission of The Bahamas ("the Commission") interprets and will supervise the obligations of licensees and registrants under the Digital Assets and Registered Exchanges Act ("registrants") in respect of the information that must accompany transfers of digital assets — the requirements known internationally as the "Travel Rule".

1.2 Registrants' obligations arise under rule 4(2) of the Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering the Financing of Terrorism and Countering the Financing of Proliferation) Rules, 2022 ("the DARE AML Rules"), which requires compliance with the Financial Transactions Reporting (Wire Transfers) Regulations, 2018 ("the Wire Transfers Regulations"), read with the record-keeping, monitoring and risk-rating provisions of the DARE AML Rules. This Note is guidance: it does not create new obligations, and it does not modify the Rules or the Regulations. It states how the Commission reads the existing obligations as applied to digital asset transfers, consistently with the FATF Standards, and what the Commission will look for in supervision and examinations.

1.3 This Note is issued following approval by the Executive Director. The Commission is progressing amendments to the DARE AML Rules to state these requirements in digital-asset-native terms; this Note applies in the interim and will be revised or withdrawn upon the amendments taking effect.

1.4 This Note applies to every registrant that sends, receives, or participates in the execution of transfers of digital assets on behalf of customers, in any role: as the ordering institution (acting for the originator), the beneficiary institution (acting for the recipient), or an intermediary.

1.5 Transfers between two customers of the same registrant that are settled on the registrant's own books, with no transfer between institutions, are not digital asset transfers for the purposes of this Note. The registrant's ordinary customer due diligence, monitoring and record-keeping obligations continue to apply to such internal movements.

Part II — The Core Obligation

2.1 When a registrant conducts a digital asset transfer on behalf of a customer, required information about the originator and the beneficiary must be collected, held, and transmitted to the institution on the other side of the transfer. The threshold and information requirements of the Wire Transfers Regulations apply, read for the digital asset context as follows: references to an "account number" or "unique transaction identifier" include the wallet address used to process the transfer; and the transfer value threshold of one thousand dollars (USD/EUR 1,000, or its equivalent in another currency, in accordance with the FATF standard, or its foreign currency or digital asset equivalent at the time of the transfer) applies.

2.2 The required information is:

	Transfers of USD/EUR 1,000 (or its equivalent) or more	Transfers below USD/EUR 1,000 (or its equivalent)
Originator	Name; wallet address or account number used to process the transfer; and one of: physical address, national identity number, customer identification number, or date and place of birth	Name; and wallet address or account number
Beneficiary	Name; and wallet address or account number	Name; and wallet address or account number
Verification	Ordering registrant verifies its own customer's information; beneficiary registrant verifies the beneficiary's identity where not previously verified	No verification required unless there is suspicion of money laundering, terrorism financing or proliferation financing

2.3 The required information does not need to be recorded on the blockchain or attached to the on-chain transaction. It must be transmitted between the institutions, through a secure channel, as described in Part III.

2.4 Occasional transactions at or above the threshold attract the customer due diligence obligations of the DARE AML Rules in the ordinary way; nothing in this Note reduces those obligations.

2.5 Registrants should be aware that counterparties in jurisdictions applying stricter standards — including the European Union, where no de minimis threshold applies to transfers between institutions — may transmit, and may lawfully require, information for transfers below USD/EUR 1,000 (or its equivalent) and beyond the Bahamian minimum. Providing such information is permitted, and registrants should be prepared to receive and handle it in accordance with Part VII.

2.6 The threshold is not an avoidance device. Deliberately splitting a transfer, or structuring a series of transfers, so that individual amounts fall below the threshold does not relieve the obligations that would attach to the full amount, and is itself an indicator of potential illicit activity which the registrant's monitoring systems are expected to detect (see the AML/CFT/CPF Guidance Notes' red-flag expectations). The Commission will treat patterns of just-below-threshold transfers as a supervisory concern.

Part III — Transmission: Immediately and Securely

3.1 The ordering registrant must submit the required information to the beneficiary institution immediately — meaning before or simultaneously with the transfer itself, and not on a deferred or on-request basis — and securely, meaning through a channel that protects the confidentiality and integrity of the information in transit and at rest.

3.2 The Commission does not mandate any particular travel rule messaging solution. Registrants may use any protocol or commercial solution that achieves complete, immediate and secure transmission and supports the registrant's record-keeping obligations. Registrants should assess and document the interoperability of their chosen solution with the solutions used by their principal counterparties, and should not treat a counterparty's use of a different solution as excusing non-transmission. Responsibility for compliance rests with the registrant at all times and cannot be outsourced to a solution provider. The outsourcing requirements of the AML/CFT/CPF Guidance Notes — due diligence, mandatory contractual provisions, immediate availability of information to the registrant and the Commission, and prior notification to the Commission of material outsourcing arrangements — apply with particular force to travel rule messaging providers.

3.3 The three-business-day on-request model available for domestic fiat wire transfers under the Wire Transfers Regulations is not an appropriate reading for digital asset transfers, which the Commission treats as requiring immediate transmission in all cases given their inherently cross-border character.

3.4 A registrant acting as an intermediary in a chain of transfers must ensure that all originator and beneficiary information received accompanies its onward transfer. Where technical limitations prevent this, the registrant must retain all information received for at least five years and provide it promptly on request to the beneficiary institution or the Commission.

Part IV — Counterparty Due Diligence and the Sunrise Issue

4.1 Before conducting a transfer, a registrant should take reasonable steps to determine whether the counterparty wallet is hosted by an institution or is an unhosted wallet, since the applicable obligations differ and misidentification of the wallet's nature is itself a source of compliance failure. Determination methods include analytics attribution, counterparty and solution-network directories, and enquiry of the customer.

4.2 Before transmitting travel rule information, a registrant should satisfy itself that the counterparty institution: (a) is subject to anti-money laundering and countering the financing of terrorism obligations in its jurisdiction; and (b) can reasonably be expected to protect the confidentiality and integrity of the information. Counterparty assessments should be documented, reviewed periodically, and refreshed on adverse information.

4.3 Where a counterparty is in a jurisdiction that has not yet implemented or is not yet enforcing Travel Rule requirements, the registrant must in every case take reasonable steps to establish whether the counterparty can receive the required information and, where it cannot, must still collect, verify and store the required information before making the transfer. The risk-based decision is confined to whether and on what terms to execute, and measures may include enhanced monitoring of the relationship and its transactions; limiting the products, volumes or exposure transacted with the counterparty; or declining the transfer or the relationship. A registrant's policies must state how it treats such counterparties; silence is not a policy.

Part V — Transfers Involving Unhosted Wallets

5.1 Where a customer transfers digital assets to, or receives digital assets from, an unhosted wallet (a wallet not held with any institution), there is no counterparty institution to transmit to or receive from. In every such case — at any value — the registrant must obtain from its own customer the required originator and beneficiary information, including the name and identifying information of the counterparty associated with the unhosted wallet; must conduct a risk assessment of the wallet address (in real time, or post-transaction where the registrant's risk framework so provides); must screen the address and the counterparty details in accordance with Part VIII; and must hold the information in accordance with Part VII. This standard conforms to the AML/CFT/CPF Guidance Notes, and to rule 3(k) of the DARE AML Rules, which identifies unhosted wallets as a source of potential risk to be identified and mitigated.

5.2 The registrant must refuse, suspend or terminate a transfer involving an unhosted wallet where the customer cannot or does not provide the required counterparty details; where the address is linked to illicit activity, sanctions targets or unauthorised mixing services; or where the risks cannot be effectively mitigated. Above that mandatory floor, and depending on the registrant's risk rating framework, enhanced measures for unhosted wallet exposure may include verification of the customer's control of the unhosted wallet, blockchain analytics screening of the wallet consistent with rule 18(2)(c), and transaction limits.

5.3 Verification of a customer's ownership or control of an unhosted wallet is risk-based, but sole reliance on the customer's self-declaration is not sufficient to establish ownership or control. Where corroboration is warranted, methods include the signing of a specified message, a transfer of a predefined amount between the wallet and the customer's account, and analytics attribution.

Commission's Expectations — Counterparties and Unhosted Wallets

- Documented decision logic, tested in practice, for determining whether a counterparty wallet is institution-hosted or unhosted.
- Counterparty due diligence records grounded in primary sources, including home-regulator register extracts with dates.
- For every unhosted wallet transfer: the counterparty information obtained, the risk assessment, the screening result, and — where applicable — the refusal, suspension or termination record.
- For sunrise counterparties: evidence that the required information was collected, verified and stored before the transfer, and the recorded basis for executing or declining.

Part VI — Receiving Transfers: Detection and Response

6.1 A registrant receiving digital asset transfers must take reasonable measures — which may include real-time or post-event monitoring — to detect transfers that arrive without the required originator or beneficiary information, or with information that is incomplete or meaningless (such as placeholder entries), or whose transmitted originator or beneficiary identifiers conflict with verified on-chain attribution.

6.2 A registrant must adopt and document risk-based policies and procedures that determine when it will execute, reject, suspend or return a transfer lacking required information, and the follow-up action it will take, including requesting the missing information from the ordering institution and setting the period within which a response is expected. In determining the treatment of a transfer lacking required information, the registrant should have regard to the status of Travel Rule implementation in the counterparty's jurisdiction, including the Commission's maintained designation of enforcing and non-enforcing jurisdictions as applied in the quarterly Travel Rule Compliance Return. Where detection under this Part indicates potential money laundering, terrorist financing or proliferation financing, the registrant should place a temporary operational hold on the affected transfer pending its internal investigation, and report in accordance with the AML/CFT/CPF Guidance Notes where grounds for suspicion are confirmed.

6.3 Where an ordering institution repeatedly fails to supply required information, the registrant's policies should provide for escalation, which may include restricting or terminating the relationship, and consideration of whether the pattern gives rise to a suspicious transaction reporting obligation.

6.4 Missing, incomplete or implausible travel rule information is a factor the registrant must weigh in deciding whether a transaction is suspicious. Where a suspicious transaction report is made, the registrant must not disclose that fact to the counterparty or customer.

6.5 A transfer that is returned or refunded is a new digital asset transfer, attracting the obligations described in this Note in its own right, with the returning registrant as the ordering institution.

Commission's Expectations — Receiving-Side Handling

- Alert outputs for missing, incomplete, meaningless and chain-conflicting information, each with a recorded disposition.
- Timestamped evidence of temporary operational holds and of the follow-up requests made to ordering institutions, with response periods stated in policy.
- Suspicious transaction reporting decisions evidenced, with tipping-off discipline observed.
- Returned transfers treated as new transfers, with the obligations discharged in that capacity.

Part VII — Records

7.1 All information collected, received and transmitted under the obligations described in this Note must be retained for at least five years, in accordance with rules 19 to 21 of the DARE AML Rules and the Wire Transfers Regulations. Transaction records must include the public keys or equivalent identifiers of the relevant parties (rule 20(e)), and should include the travel rule messages sent and received, counterparty assessments under Part IV, and the disposition of any transfer lacking required information under Part VI.

7.2 Records must be retrievable in a form that permits the Commission, in supervision or examination, to reconstruct any given transfer: the parties, the wallets, the information transmitted or received, the channel used, and the decisions taken.

Part VIII — Sanctions Screening

8.1 Registrants must screen the parties to digital asset transfers, and the associated wallet addresses, against applicable targeted financial sanctions, including those relating to terrorism financing and proliferation financing, in accordance with their obligations under Bahamian law, and must not execute a transfer involving a designated person or entity. Screening should occur before execution and on the receipt of transfers, and the registrant's policies should address the treatment of transfers connected to designated persons, including freezing and reporting obligations.

Part IX — Supervision

9.1 The Commission will supervise compliance with the obligations described in this Note through its ongoing supervisory programme and on-site examinations, including: review of registrants' travel rule policies and solution arrangements; testing of transfer samples for completeness and timeliness of information sent and received; testing of detection and response arrangements for incoming transfers; review of counterparty assessments and unhosted wallet controls; and review of records under Part VII.

9.2 Registrants should notify the Supervision Department of the travel rule messaging solution or arrangements they have adopted, and of any material change to those arrangements, so that the Commission's supervisory records remain current.

9.3 A registrant's travel rule policies and procedures should be approved by senior management, supported by training for relevant staff, and subject to periodic testing or independent review. The Commission will look for evidence of each in supervision.

9.4 Registrants report quarterly on travel rule compliance in the form prescribed by the Commission (Form TRR-1), issued under the Travel Rule Compliance Monitoring Programme on the collection basis of section 32(1)(b) of the Digital Assets and Registered Exchanges Act, 2024, and notified by industry notice. The Return's requirements — including the compliant-transaction proportions by value and number, and exposure to unregulated counterparty institutions — are stated in the notice, and completeness and accuracy of Returns are themselves supervisory expectations.

Commission's Expectations — Governance and Reporting

- Travel rule policies approved by senior management, with training and periodic testing or independent review evidenced.
- The Commission notified of the messaging solution in use and of material changes, with the notification current.
- Quarterly Returns complete, accurate and reconcilable to the registrant's own records.

9.5 Registrants should direct questions on this Note to the Supervision Department. This Note will be kept under review and revised as the legislative framework and the FATF Standards evolve.