FSU
Financial Services Unit

GUIDANCE NOTES

2025

FOR VIRTUAL ASSET SERVICE PROVIDERS

LEARN ABOUT

- Overview of FATF Compliance
- Key Regulatory Responsibilities
- Risk and Compliance Framework

APPROVED
30/1/2025
Director, Financial Services Unit
Ministry of Finance
Commonwealth of Dominica

CERTIFIED
30/1/2025
Director, Financial Services Unit
Ministry of Finance
Commonwealth of Dominica

INTRODUCTION

The Financial Action Task Force (FATF) introduced the 'Travel Rule' in 2019 by way of a revision to Recommendation 15 to extend anti-money laundering, counter terrorist financing and counterproliferation financing obligations to virtual assets (VA) and Virtual Assets Services Providers (VASPs). The amendment to the recommendation required countries to identify and assess their money laundering (ML) and terrorist financing (TF) related risks for new, developing and preexisting technologies. Further updates and reports by the FATF resulted in the revision of Recommendation 16, which also impacts VASPs. FATF Recommendations 15 (New Technologies) and 16 (Wire Transfers) were updated because of the advancement of new technologies and wire transfers are of particular importance to VASPs. FATF's amendments to Recommendations 15 and 16 together with Interpretive Notes brought VASPs into scope for compliance with AML/CFT obligations.

Therefore, VASPs must assess their ML, TF and PF risks posed by counterparty VASPs which requires due diligence assessments of those counterparty VASPs. VASPs in scope of Dominica are required to be registered/Licensed in accordance with the Virtual Assets Services Providers Act, 2022 (the "Act") and comply with all relevant laws.

Virtual Asset Service Providers play a critical role in the financial ecosystem. To ensure market integrity, consumer protection, and the prevention of financial crimes, VASPs must adhere to regulatory frameworks and international standards.

This guidance provides an overview of key obligations and expectations for VASPs; and provides clarification on the requirements for VASPs to comply with the Travel Rule. This guidance does not replace any previously issued law or guidance.This Guidance should be read together with the Virtual Asset Business Act and Virtual Asset Business Regulation, Money Laundering, Terrorist Financing and Proliferation Financing and other relevant laws and regulations applicable to VASPs.

Obligations of Directors and Senior Officers

Directors and Senior Officers of Dominica registered VASPs are responsible for ensuring compliance with the AMLTFCoP, and other applicable laws.In addition, Directors and Senior Officers of VASPs are reminded of the requirements under Section 12 of the Act to ensure VASP compliance with relevant laws, "including compliance with other enactments relating to anti-money laundering and counter financing of terrorism legislation." As such, Directors and Senior Officers must ensure that their governance framework provides for effective oversight and implementation that ensures compliance with the Travel Rule (FATF Rec 16).

Application of the FATF Travel Rule to VASPs

In the conduct of their operations, VASPs must:

- be able to demonstrate that reasonable steps have been taken and controls implemented to ensure compliance with the Travel Rule. This can include the VASP's documented AML/CFT policies, procedures and controls. A VASP may use a third-party service provider (Travel Rule Service Provider) to implement and operationalize the Travel Rule requirements. However, the VASP must, before it engages the service provider, and during the relationship ensure that the provider is appropriately risk assessed. The Unit, in its assessment of a VASP during its application for licensing, upon registration and as part of its ongoing supervision, requires full disclosure of any data or other information in relation to a Travel Rule service provider with whom a VASP has entered into an agreement with.

Where VASPs send virtual assets to a jurisdiction without full Travel Rule implementation, it is expected that VASPs will

- take all reasonable steps to determine whether the recipient VASP can properly receive the required information.

- collect and retain all information relating to transactions where the recipient VASP cannot receive the required information, which is to be made available to the Unit and the relevant competent authorities and law enforcement agencies upon request and without delay.

When receiving a virtual asset transfer from a jurisdiction without the Travel Rule

- where a virtual asset transfer is missing information or the information provided is incomplete, the Dominica registered VASP should consider the jurisdiction in which the originator VASP operates and the status of Travel Rule implementation in that jurisdiction.

- a VASP should consider all relevant factors such as status of travel rule, missing information, geographic and country risk etc. in its risk assessment prior to deciding whether funds are made available to the intended beneficiary.

• VASPs may use blockchain analytics to inform their risk assessments of VASPs operating in jurisdictions without the Travel Rule.This does not negate the requirements for VASPs operating in the jurisdiction to achieve compliance with their AML/ CFT/CPF obligations, which includes reporting suspicious transaction reports (STRs) to the Financial Intelligence Unit (FIU).

Required information that must accompany an inter-VASP transfer

Originator VASPs should ensure the following information accompanies all transfers with sufficient detail to ensure that all relevant parties including originator and beneficiary can be readily identifiable.

a) The name and address of the originator
b) The registered or trading names where the originator or beneficiary is a legal structure
c) The account number of the originator where the account is used to process a transaction and the account number of the beneficiary or other unique transaction identifiers
d) The originator's date and place of birth; or the customer identification number or national identity number of the payer

It is the responsibility of a VASP to ensure that they have appropriate and effective policies, procedures and controls to detect missing or inaccurate information including that related to the beneficiary and to respond accordingly. VASPs must periodically test and record findings of the robustness of these systems. It is expected that the provision of the required information by the originator VASP occurs before or at the moment the transaction is completed. The transaction is completed when the recipient VASP makes the virtual assets available to the beneficiary

Transaction Threshold

- When assessing whether a transfer is equal to our exceeds the USD 1,000, VASPs should take the USD value recorded at the time of the transfer is executed by the originator.
- Transfers of funds not exceeding USD 1,000 should be subject to scrutiny on a risk-based approach to assess whether the funds to be transferred are , connected to criminal activity or appear to be structured to evade detection of money laundering, terrorist financing, or proliferation financing.

- Aggregated transactions from the same or connected originator to the same or connected beneficiary over a short period of time should be considered as linked transactions. It is expected that VASPs will have policies, procedures and controls in place to detect potentially linked transactions.

- The characteristics of the transactions should be assessed and considered when identifying linked transactions. For example, where several payments are made to the same recipient from one or more sources over a short period of time, or where a customer regularly transfers funds to one or more sources. For lower-risk situations, a longer period of time (such as 3 to 6 months) for linking transactions may be more appropriate, provided that this is not a common occurrence.

Examples of In-scope transfers

- Intragroup transfers (those transfers between different legal entities within the same group).
- Transfer between VASPs where the originator and beneficiary are the same person (for example, an individual has established accounts with two or more VASPs).

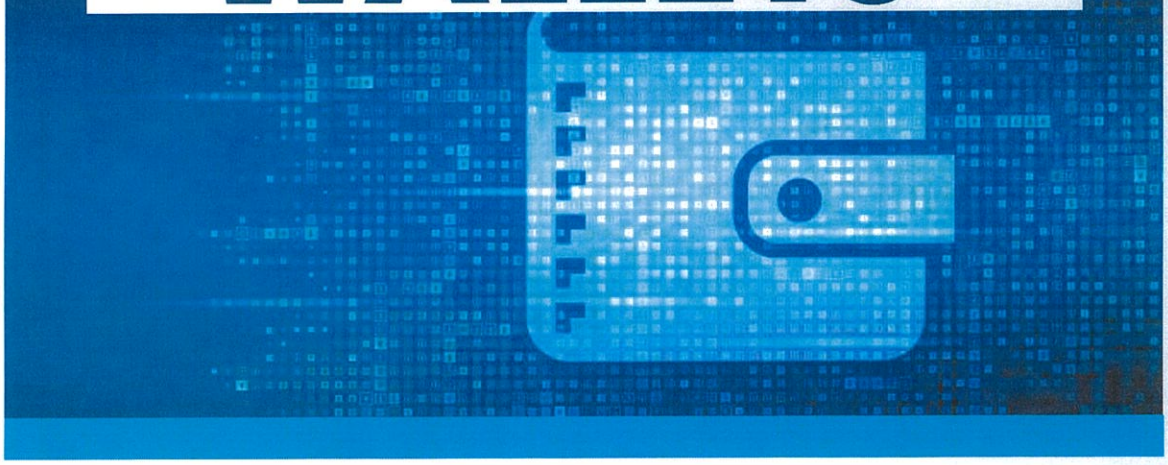
Examples of Out-of-scope transfers

- Transfers where both the originator and beneficiary hold accounts with the same VASP
- Transfers between two VASPs acting on their own behalf.
- Transfers of funds not exceeding USD 1,000 unless there are reasonable grounds for suspecting that the funds to be transferred are connected to money laundering, terrorist financing or proliferation financing activities.

Intermediary VASPs

- An "intermediary VASP" is a service provider that participates in the execution of a transfer of virtual assets and is not the originating VASP or the beneficiary VASP; Alternate definition: An "intermediary VASP" is a service provider that participates in the execution of a transfer of virtual assets but does not have a business relationship with either the originator or the beneficiary.
- It is the responsibility of the intermediary VASP to check whether all information required has been received before completing the transfer of virtual assets. Where information is missing or incomplete, it is expected that the intermediary VASP will consider whether to delay the onward transfer until the information is received. This consideration should follow a risk-based approach and be sufficiently documented such that all Competent Authorities can understand why the transfer of virtual assets was either completed or delayed/refused.
- It is expected that the intermediary VASP will send on any requested information which is received after it has transferred the virtual asset, as soon as is practicable, to a receiving VASP.

UNHOSTED WALLETS



Ensuring Beneficial Ownership and Control

Transfers to/from unhosted wallets

An unhosted wallet is a wallet not hosted by a VASP.

- VASPs should adopt a risk-based approach when dealing with unhosted wallet transfers.

- In arriving at the risk rating from an unhosted transfer of virtual assets the VASP may take into account:

a) The purpose and nature of the business relationship with the owner/beneficial owner of the unhosted wallet.
b) The jurisdiction of the unhosted wallet.
c) The value and/or frequency of the transfer(s)/linked transfers to/from the unhosted wallet.
d) Outputs from Blockchain Analytics solutions detailing any association of the unhosted wallet with illicit activities.
e) Information the VASP obtained during the establishment of the business relationship and/or during the relationship with the customer.

In higher risk cases, VASPs should also consider further steps to verify the ownership and control of the unhosted wallet. This can include additional verification methods, such as the 'Satoshi Test', where a small amount of virtual assets is to be sent to a specified wallet address, or through 'Address Ownership Proof Protocol', which allows a VASP to verify the ownership of an unhosted wallet. VASPs may use other measures that allow for robust verification to ensure that they validate ownership and control of an unhosted wallet.

Where a VASP does not obtain sufficient information to be comfortable with the ownership and control of the unhosted wallet, the virtual assets should not be made available to the intended beneficiary. Additionally, a VASP should determine whether the activity raises suspicion of ML, TF, PF or other criminal activity and file a suspicious transaction report to the FIU without delay.

1. Legal and Regulatory Compliance

Licensing and Registration:

- Obtain necessary licenses or registration with the relevant authority in your jurisdiction.
- Keep registration details updated and report changes promptly.

AML/CFT Requirements:

- Comply with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations, in line with Financial Action Task Force (FATF) recommendations.
- Conduct thorough risk assessments and implement a risk-based approach to manage exposure to illicit activities.

Travel Rule Compliance:

·Ensure that originator and beneficiary information is exchanged with other VASPs or financial institutions for virtual asset transactions exceeding the designated threshold.

2. Customer Due Diligence (CDD)

- Implement CDD processes to verify the identity of customers, beneficial owners, and, where applicable, third parties.
- Monitor transactions continuously for unusual or suspicious activity and maintain robust systems for transaction monitoring.
- Establish enhanced due diligence (EDD) for higher-risk customers or transactions.

3. Reporting and Record-Keeping

- File Suspicious Transaction Reports (STRs) with the relevant authority when transactions appear to involve illicit activity.
- Maintain transaction and CDD records for the period required by law, ensuring they are secure and retrievable.

4. Governance and Internal Controls

- Establish clear governance structures with defined roles and responsibilities for compliance. Appoint a compliance officer and Alternate CO to oversee AML/CFT obligations.
- Train staff regularly on compliance requirements and emerging risks.

5. Technology and Cybersecurity

- Use secure and reliable technology to facilitate operations and safeguard virtual assets
- Implement robust cybersecurity measures, including multi-factor authentication, data encryption, and regular penetration testing.
- Develop incident response plans to address potential data breaches or system failures.

6. Consumer Protection

- Disclose all fees, risks, and terms of service clearly to customers. Ensure that marketing materials are not misleading and comply with local advertising regulations.
- Establish grievance mechanisms to address customer complaints effectively.
- Implement educational campaigns addressing VA risks, fraud prevention, and responsible use.

7. Cross-Border Operations

- Understand and comply with the regulatory requirements of jurisdictions in which you operate.
- Partner with other VASPs and financial institutions that have robust compliance frameworks.

8. Penalties for Non-Compliance

- Non-compliance with regulatory obligations can result in severe penalties, including:

Fines/ Penalties.

- License suspension or revocation
- Criminal charges for executives or staff involved in misconduct

9. Resources and Further Guidance

For more information on compliance standards and best practices, refer to:

- Financial Action Task Force (FATF) Guidance on Virtual Assets and VASPs
- The Financial Services Unit Website www.fsu.gov.dm

DEFINITIONS/GLOSSARY

AML	Anti-Money Laundering
AMLTFCOP	Anti-Money Laundering and Terrorist Financing Code of Practice-2014
AMLR	Anti-Money Laundering Regulations
CFT	Countering the Financing of Terrorism
CPF	Counter Proliferation Financing
FATF	Financial Action Task Force, which is the international standard setter for Anti-money Laundering (AML), Counter-terrorist Financing (CFT) and Counter-proliferation Financing standards
FATF TRAVEL RULE	The requirement developed by FATF that sets out the need for VASPs to collect originator and beneficiary information for transfers of virtual assets as a part of their AML/CFT/CPF compliance framework
HASH NUMBER	A number generated from a cryptographic hash function
OTC	Over the Counter
STR	Suspicious Transaction Report
UNHOSTED WALLET	A wallet not hosted by a VASP
VIRTUAL ASSETS	A digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, but does not include (a) digital representations of fiat currencies and other assets or matters specified in the Guidelines; or (b) a digital record of a credit against a financial institution of fiat currency, securities or other financial assets that can be transferred digitally.
VIRTUAL ASSET SERVICE	The business of engaging, on behalf of another person, in any VASP activity or operation (as outlined in the definition of "VASP"), and includes (a) hosting wallets or maintaining custody or control over another person's virtual asset, wallet or private key; (b) providing financial services relating to the issuance, offer or sale of a virtual asset; (c) providing kiosks (such as automatic teller machines, bitcoin teller machines or vending machines) for the purpose of facilitating virtual assets activities through electronic terminals to enable the owner or operator of the kiosk to actively facilitate the exchange of virtual assets for fiat currency or other virtual assets; or (d) engaging in any other activity that, under guidelines issued pursuant to VASPS ACT 2022, constitutes the carrying on of the business of providing virtual asset service or issuing virtual assets or being involved in virtual asset activity.