ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Travel Rule (Transfer of Virtual Assets) Code 2024

Guidance Notes

December 2024

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

Version history

Version 1	December 2024

1. Foreword

This guidance is applicable to businesses conducting Virtual Asset Service Provider ("VASP") activity, which includes the activity of an Intermediary Virtual Asset Service Provider ("IVASP").

The activity of a VASP is included in paragraph 2(6)(r) of Schedule 4 to the Proceeds of Crime Act 2008 ("POCA") and is defined as follows: -

"virtual asset service provider" or **"VASP"** means any natural or legal person who *by way of business* conducts one or more of the following activities or operations for or on behalf of another natural or legal person **–**

a. exchange between virtual assets and fiat currencies;
b. exchange between one or more forms of virtual assets;
c. transfer of virtual assets;
d. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
e. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

The activity of an IVASP is included in paragraph 4 of the Travel Rule (Transfer of Virtual Assets) Code 2024 ("the Travel Rule Code") and is defined as follows:

"**intermediary virtual asset service provider**" means a virtual asset service provider that provides exchange, transfer or safekeeping and/or administration services to, or for, the virtual asset service provider of the originator or beneficiary but does not have a business relationship with either the originator or the beneficiary.

A business conducting VASP activity as defined in Schedule 4 to POCA, is subject to both the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the AML/CFT Code") and the Travel Rule Code. This sector also falls under the Designated Businesses (Registration and Oversight) Act 2015 ("the DBROA") and is therefore subject to the registration requirements of that Act. The Financial Services Authority ("the Authority") is responsible for overseeing this sector for Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") purposes. A full list of the designated business activities can be found in Schedule 1 to the DBROA.

The purpose of this guidance document is to provide relevant persons that are conducting VASP activity - as registerable under the provisions of the DBROA – with an overview of their obligations in respect of Travel Rule. This guidance

should be read in conjunction with the Travel Rule Code, the VASP sector specific guidance, the AML/CFT Handbook and the AML/CFT Code.

Any person seeking to provide the services of a VASP, in or from the Isle of Man should obtain relevant independent legal advice to ensure that the proposed activities are subject to the appropriate framework i.e. whether the activity is designated business under the DBROA or licensable under other legislation such as the Financial Services Act 2008.

2. Introduction

This guidance relates to the provisions of the Travel Rule Code 2024 and will be a living document that is regularly reviewed. This guidance should be read in conjunction with the VASP guidance, which is due to be fully updated following the completion of the Island's National Risk Assessment.

The virtual asset industry is evolving rapidly, and with continued global adoption comes the increasing use of virtual assets as a viable form of payment and value transfer. As the usability and viability of virtual assets (as a mainstream solution for value transfer) increases, the risks that the technology could be exploited for criminal purposes also increases.

As such, there is a need to continually develop our regulatory framework in line with globally recognised international standards. The implementation of Travel Rule is a fundamental component of the framework for the virtual asset sector and is key to reducing the facilitation of Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF") through virtual assets.

The Financial Actions Task Force's ("FATF") Recommendation 16[1] ("R16") sets out the requirements for the provision of originator and beneficiary information in respect of wire transfers.

Colloquially known as the Travel Rule, R16 was originally developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available to:

[1] FATF Methodology - https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.coredownload.pdf

a. law enforcement agencies
b. financial intelligence units
c. ordering, intermediary and beneficiary financial institutions.

In 2019 the FATF expanded the scope of R16 to introduce the requirements for entities operating in the VASP sector to obtain unique originator and beneficiary customer information when processing virtual asset (VA) transactions.

The primary purpose of the Travel Rule Code is to implement the requirements for VA transfers to be accompanied by certain identifiable information on the originator (*the individual who owns and allows the transfer of the VA*) and the beneficiary (*the intended recipient of the VA*).

A relevant person must take all reasonable measures to ensure they comply with the requirements of the Travel Rule Code. The Travel Rule Code includes details of penalties that may be applied to VASPs should instances of material and significant non-compliance be identified.

The Travel Rule Code is designed to sit alongside the AML/CFT Code, and forms part of the wider obligations for relevant persons engaged in VASP activity to have effective procedures and controls in place to detect and prevent ML/TF/PF.

3. Terminology

Code 4(1)

There are several different terms and definitions used when describing concepts within this sector. The following definitions are used within this guidance document and are largely taken from globally recognised sources such as FATF:

Virtual Asset Service Provider (please see section 1 of this document for the Isle of Man's legislative definition of this term).

Virtual Asset refers to a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities, and other financial assets.

Travel Rule Code refers to the Travel Rule (Transfer of Virtual Assets) Code 2024 which obliges relevant persons undertaking the activities of a VASP to transfer and retain certain specified customer information in accordance with the FATF's Recommendation 16.

4. The Originator

Code 5

Originator refers to the account holder who allows a VA transfer from an account in their control, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the VA transfer.

The originator of the VA must ensure that the below information accompanies all VA transfers:

Code 5(2)

(a) the name of the beneficiary;
(b) the unique account identifier of the beneficiary;
(c) the name of the originator;
(d) the unique account identifier of the originator;
(e) where the beneficiary or originator does not have a unique account identifier, a unique transaction identifier; and
(f) one of the following -

i. the originator's address;
ii. a national identification number of the originator; or
iii. the originator's date and place of birth.

Code 5(5)

The originating VASP must also ensure that the information provided for 'its' customer is verified as "**accurate"** and is consistent with its own records in respect of the originator's name and, where applicable, the originator's unique account identifier (please see Section 6 for more information).

Code 4(1)

"**accurate**" means information that has been verified for accuracy.

Code 5(1)(a) & (b)

The information must be transferred '*immediately*' and '*securely*':

- '*immediately*' means that providers should submit the required information prior, simultaneously or concurrently with the transfer itself.
- '*securely*' means that the information should be transmitted and stored in a secure manner.

5. The Beneficiary

Code 6

Beneficiary refers to the natural person, legal person or legal arrangement who is identified by the originator as the intended recipient of the requested VA transfer.

The beneficiary of a VA must ensure that the below information is received for all VA transfers:

Code 5(2)

(a) the name of the beneficiary;
(b) the unique account identifier of the beneficiary;
(c) the name of the originator;
(d) the unique account identifier of the originator;
(e) where the beneficiary or originator does not have a unique account identifier, a unique transaction identifier.

Code 4(1)

The beneficiary VASP must also ensure that the information received for 'its' customer is verified as "**accurate**" and is consistent with its own records in respect of the beneficiary's name and, where applicable, the beneficiary's unique account identifier (please see Section 6 for more information).

6. Data Accuracy and Verification

Code 4(1)

The Travel Rule Code stipulates there is a requirement for certain elements of specified customer information to be "**accurate**", when facilitating a VA transfer.

The below table sets out the Authority's expectations in respect of data accuracy, and outlines the respective obligations that both the originator and the beneficiary must adhere to when facilitating a VA transfer:

Data item / Actions required	**Ordering VASP**	**Beneficiary VASP**
Originator information	All information specified in paragraph 5(2) of the Travel Rule Code is required for submission to the beneficiary VASP. This information must be **accurate** i.e. the information should be verified for accuracy by the ordering VASP as part of their Customer Due Diligence ("CDD") process.	The beneficiary must obtain all the information specified in paragraph 5(2) of the Travel Rule Code from the ordering VASP. Data accuracy is **NOT** explicitly required by the Travel Rule Code. The beneficiary VASP can assume that the information has been verified for accuracy by the ordering VASP as part of their CDD process.
Beneficiary information	All information specified in paragraph 5(2) of the Travel Rule Code is required for submission to the beneficiary VASP.	The beneficiary VASP must obtain all the information specified in paragraph 5(2) of the Travel Rule Code from the ordering VASP.

	Data accuracy is **NOT** explicitly required by the Travel Rule Code. The ordering VASP must, however, monitor to confirm that no suspicions arise.	This information must be **accurate** i.e. the beneficiary VASP must have verified the necessary data pertaining to its customer and needs to confirm if the data received is consistent with its own customer records.
Actions required	Obtain the necessary information from the originator and retain a record. Screen to confirm that the beneficiary is not sanctioned. Monitor transactions and report when a suspicion of ML/TF/PF arises.	Obtain the necessary information from the ordering VASP and retain a record. Screen to confirm that the originator is not sanctioned. Monitor transactions and report when a suspicion of ML/TF/PF arises.

Further information in respect of obligations relating to Customer Due Diligence and Record Keeping can be found in part 10 of this guidance document and paragraph 9 of the Travel Rule Code.

7. Scope of the Travel Rule Code

There are instances where the transfer of VA's may be out-of-scope of the Travel Rule Code. Below is a list of VA transfers that would typically fall outside the of the requirements of the Travel Rule Code:

- transfers where both the originator and the beneficiary hold accounts with the same VASP;
- transfers where the originator and beneficiary are the same person and hold multiple accounts at the same VASP;
- transfers between two VASPs who are acting on their own behalf;

All other VA transfers are to be treated as 'in-scope' of the Travel Rule Code and are therefore subject to the requirements as prescribed within the Travel Rule Code.

8. Unhosted Wallets

Code 7 It is acknowledged that relevant persons undertaking the activities of a VASP may from time to time facilitate VA transfers with non-obliged entities i.e. unhosted wallets.

Relevant persons should be aware of the increased risks of undertaking VA transactions to/from unhosted wallets. Due to the relative anonymity of transactions involving unhosted wallets, use of these can be attractive to illicit actors as a way of moving funds quickly, without limits and without being fully identifiable.

It is highly recommended that where a firm facilitates transactions involving unhosted wallets the risks of this activity are continually assessed as part of the firm's Business Risk Assessment.

In instances where a relevant person does facilitate a VA transfer with an unhosted wallet, the relevant person must obtain from their customer (whether originator or beneficiary) the information specified in paragraph 5(2)(a) to (e) of the Travel Rule Code.

Paragraph 5(2)(f)[2] of the Travel Rule Code is disapplied for transactions involving unhosted wallets.

Where high risk indicators are observed in transactions utilising unhosted wallets, the relevant person must consider obtaining additional information on the unhosted wallet user.

In assessing the level of risk arising from an unhosted wallet transfer, the relevant person must take into account the following factors:

- the value of the transfer, and any linked transfers;
- source of funds;
- the purpose and nature of the business relationship with 'its' customer and the unhosted wallet transfer;
- the jurisdiction (if known) of the unhosted wallet;
- the frequency of transfers made by or to the customer, to or from the unhosted wallet;
- the duration of the business relationship with the customer; and
- any output from Blockchain Analytics solutions used by the VASP, which might detail any association of the unhosted wallet with illicit activities.

Failure to acknowledge the increased risks associated with unhosted wallets, and provide suitable mitigations for these risks, could result in firms being exploited for criminal purposes.

Where a relevant person does not obtain the specified information to be comfortable, the transferred VA should not be made available to the intended beneficiary.

Further, where a suspicion is held the relevant person must submit an internal disclosure in accordance with paragraph 26 of the AML/CFT Code.

[2] 5(2)(f) includes the following additional information:

i. the originator's address;
ii. a national identification number of the originator; or
iii. the originator's date and place of birth.

9. *De minimis* transfers

Code 8 The inclusion of the *de minimis* transfer threshold of EUR 1000 or currency equivalent' within the Travel Rule Code is intended to reduce the amount of information required to be transferred with a VA transaction in certain circumstances.

Code 8(1) The *de minimis* does not exempt a VA transfer from travelling with certain identification information, it merely reduces the amount of information required in cases where the transfer is below the threshold.

It remains a requirement under the Travel Rule Code to ensure that the below information travels with any VA transfer that is below the *de minimis* transfer threshold:

(a) the name of the beneficiary;
(b) the unique account identifier of the beneficiary;
(c) the name of the originator;
(d) the unique account identifier of the originator;
(e) where the beneficiary or originator does not have a unique account identifier, a unique transaction identifier.

Where a VA transfer is below the *de minimis* threshold, the specified information does not need be verified for accuracy. However, the relevant person should be required to verify the information pertaining to its customer where there is a suspicion of ML/TF/PF.

In the case of a VA transfer above the *de minimis* threshold, relevant persons should ensure that data accuracy requirements are consistent with those outlined for the originator and beneficiary in part 6 of this guidance document.

10. Sunrise Issue and interoperability

The FATF have acknowledged in their guidance '*FATF Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*[3]*'* that; delays in implementation and different timelines for the enforcement of the Travel Rule across jurisdictions can result in what is referred to as the 'sunrise issue'. This can present challenges for VASPs when transacting with counterparties in jurisdictions where the Travel Rule has not yet been implemented. There is an expectation that where a relevant person is engaged in a VA transfer, all reasonable measures should be taken to ensure compliance with the requirements of the Travel Rule Code.

Ultimately, the 'sunrise issue' will not be fully mitigated until there is widespread global adoption of the FATF standards on VAs and VASPs, including the universal implementation of the Travel Rule, supported by the technology needed to efficiently and effectively send, receive, collect and retain the required information.

When sending a VA to a jurisdiction that does not currently comply with the Travel Rule, relevant persons should take reasonable steps to:

- establish whether the beneficiary VASP can receive the information that travels with the VA; and
- in cases where the beneficiary VASP cannot receive the data, retain all transaction data related to the VA transfer so this can be made available to competent authorities on request.

Code 6(2)

In cases where a VA is received from a jurisdiction that does not currently comply with the requirements of the Travel Rule relevant persons should:

- take reasonable steps to identify if there is any missing or incomplete information;
- where missing or incomplete information is identified, consider the jurisdiction from which the VA is originating and its status with regards to the Travel Rule implementation;
- make a risk-based assessment using the information available to determine whether or not to make the VA available to the beneficiary; and

[3] FATF Guidance – Virtual Assets and Virtual Asset Service Providers - https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

- if there are any ML/TF/PF concerns with the VA transfer, consider raising a Suspicious Activity Report ("SAR") to the Financial Intelligence Unit ('FIU') in accordance with paragraph 27 of the AML/CFT Code.

11. Customer due diligence and record keeping

VASPs operating in or from the Island are subject to all CDD requirements (amongst other requirements) as prescribed under the AML/CFT Code.

The Travel Rule Code does not alleviate relevant persons any of the obligations to obtain CDD or Know Your Customer ("KYC") information in accordance with paragraph 8, and where applicable paragraph 15, of the AML/CFT Code.

Code 9(2) Record keeping is an essential part of being able to demonstrate compliance with the Travel Rule Code requirements. This helps to ensure criminal and terrorist property can be traced and confiscated, and persons involved can be investigated and prosecuted.

Code 9(2) Record keeping procedures and controls must be sensitive to ML/TF/PF risk and enable the relevant person to manage and mitigate their ML/TF/PF risks. Furthermore, satisfactory record keeping is paramount for relevant persons themselves in ensuring they are able to comply with their obligations under the AML/CFT legislation. A relevant person's record keeping procedures and controls must enable them to satisfy, within a reasonable time frame, any enquiries from competent authorities.

Furthermore, it is only through adequate record keeping that relevant persons can demonstrate compliance with AML/CFT legislation e.g. to the relevant person's auditors, supervisors or in the event of legal enquiries.

Record retention, storage and retrieval are also specific requirements under the Travel Rule Code.

12. Travel Rule return

As part of its oversight measures and to in order to inform both the risk profile of firms, and the Island's NRA, the Authority will periodically seek the completion of a Travel Rule Return from relevant persons undertaking the activities of a VASP.

The purpose of the Travel Rule return is to collect data from relevant persons relating to the originator and beneficiary information transferred in accordance with the requirements of the Travel Rule Code, specifically to gain information in relation to the Island's exposure to other jurisdictions where possible

This will allow the Authority to validate compliance with the Travel Rule Code and will also allow it to analyse the data for potential ML/TF/PF risk indicators connected to VA transfers with an Isle of Man nexus.

Further details and consultation in regards to the Travel Rule Return will follow in due course.

13. Offences and penalties

Code 10 Failure to comply with the Travel Rule Code will result in an offence being committed. Where an offence under the Travel Rule Code is committed, the Authority has a number of sanctioning powers available to it, which can be used proportionately depending on the severity of a breach.

Code 10(1)

Criminal penalties

The Travel Rule Code contains obligations which relevant persons must meet in relation to the prevention of ML/TF/PF. Paragraph 10 of the Travel Rule Code details the offences in relation to contraventions of the Travel Rule Code.

(1) A person who fails to comply with any requirements of this Code is guilty of an offence, and liable —

(a) on summary conviction, to custody for a term not exceeding 12 months or to a fine not exceeding level 5 on the standard scale or both; or

(b) on conviction on information, to custody not exceeding 2 years or to a fine, or to both.

(2) Sub-paragraph (2), (3), (4) and (5) of paragraph 42 of the AML/CFT Code shall apply to an offence under sub-paragraph (1) as if it were an offence under paragraph 42(1) of the AML/CFT Code.

The offences in relation to ML/TF/PF are contained in a number of other pieces of legislation:

- the POCA;
- the ATCA; and
- the TOCFRA

All Isle of Man primary legislation can be found here and all Isle of Man secondary legislation can be found here.

Travel Rule Code (Civil Penalties)

Civil penalties

The Authority is currently working on a project to develop a set of Civil Penalty regulations that will sit alongside the Travel Rule Code. Further outreach and consultation will be held in regards to this Civil Penalty regime in due course.