Jersey Financial Services Commission

Travel Rule guidance note

Issued: February 2024

Updated: November 2025

Contents

Glossary

Term	Definition
AML/CFT/CPF	anti-money laundering/countering the financing of terrorism/countering proliferation financing
FATF	The Financial Action Task Force
Travel Rule	for the purpose of this guidance note, 'Travel Rule' refers to the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 (jerseylaw.je) and requirements set out within this guidance note
unhosted wallet	an unhosted VA wallet, also known as a non-custodial wallet or a self-custody wallet, is a type of VA wallet where the private keys are fully controlled by the wallet owner, rather than being managed by a third-party service provider
virtual asset	A digital representation of value that can be digitally traded or transferred can be used for payment or investment purposes. For the purpose of the Travel Rule, stablecoins are included within the definition of a virtual asset.
Virtual Asset Service Provider	as defined in paragraph 24 of Part 4 of Schedule 2 to the Proceeds of Crime Law

1 Context

The Financial Action Task Force (**FATF**) has called on jurisdictions to swiftly implement its 'Travel Rule', which requires transfers of virtual assets to be accompanied by accurate originator and beneficiary information.

The European Union (EU) Legislation (Information Accompanying Transfer of Funds) (Jersey) Regulations 2017 (**Wire Transfer Regulations**)[1] were amended on 1 September 2023 to include Virtual Asset Service Providers (**VASPs**).

The Wire Transfer Regulations apply EU Regulation 2015/847 in Jersey. This regulation sets rules for including payer and payee information with fund transfers.

This guidance supplements Jersey's AML/CFT/CPF regime and does not amend or replace it. It should be read alongside relevant legislation and regulatory requirements, including:

› the Proceeds of Crime (Jersey) Law 1999

› the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008

› the Money Laundering (Jersey) Order 2008

› our Handbook for preventing money laundering, terrorist financing, and proliferation financing

While Jersey's current wire transfer regulations continue to implement Regulation (EU) 2015/847, it is important to note that the European Union has adopted Regulation (EU) 2023/1113. Jersey may consider updating its legislation to reflect EU 2023/1113.

2 Our guidance

We acknowledge that VASPs in different jurisdictions are at varying stages of adopting and implementing the Travel Rule. After engaging with industry to understand these challenges, this guidance sets out expectations for VASP compliance under different circumstances.

[1] EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 (jerseylaw.je)

3 VASP to VASP

3.1 We expect VASPs to:

3.1.1 demonstrate full compliance with the Travel Rule

3.1.2 have a functioning Travel Rule solution in place, where applicable, and be able to demonstrate it working effectively

3.1.3 maintain documented procedures that clearly outline how compliance is achieved and sustained

3.1.4 comply with the Travel Rule for all virtual asset transfers involving VASPs in Jersey or jurisdictions where it applies, ensuring accurate transmission and retention of required originator and beneficiary information

3.2 When sending a virtual asset transfer to a jurisdiction without the Travel Rule, we expect VASPs to:

3.2.1 take all reasonable steps to establish whether the recipient VASP can receive the required information

3.2.2 collect and retain the transaction information and have it available upon request, even where the recipient VASP cannot receive the required information.

3.3 When receiving a virtual asset transfer from a jurisdiction without the Travel Rule, we expect VASPs to:

3.3.1 consider whether there is missing or incomplete information and that the Jersey VASP consider the jurisdiction in which the originator VASP operates and the status of the Travel Rule in that jurisdiction

3.3.2 use the factors in 3.3.1 to inform a risk-based assessment as to whether these funds are made available to the intended beneficiary

3.3.3 leverage blockchain analytics solutions to inform this risk-based assessment, however the Jersey VASP remains fully responsible for achieving compliance with their AML/CFT/CPF obligations, including the raising of suspicious activity reports (SARs) where relevant

3.4 Required information to accompany an inter-VASP transfer

3.4.1 It is expected that the originator VASP ensure the following information accompanies transfers:

3.4.1.1 the name of the originator and the beneficiary

3.4.1.2 where the originator or beneficiary is a legal entity, their registered or trading names

3.4.1.3 the account number of the originator and the beneficiary, or other unique transaction identifiers

3.4.1.4 the transaction hash number (every transaction that occurs on the blockchain is recorded as a block, and each block has a unique hash)

3.4.2 additionally, where the originator is an individual, **one** of the following:

3.4.2.1 customer identification number

3.4.2.2 address

3.4.2.3 birth certificate, passport number, or national ID card number (or individual's date and place of birth)

3.4.3 where the originator is a legal entity, **one** of the following:

3.4.3.1 customer identification number

3.4.3.2 address of originator's registered office (or principal place of business)

3.4.4 It is the responsibility of the VASP to ensure that they have appropriate and effective procedures to detect missing or inaccurate information and to respond accordingly.

3.4.5 It is expected that the provision of the required information by the originator VASP occur 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.

3.5 Transaction values

3.5.1 When assessing whether a transfer is equal to or exceeds the EUR 1,000, VASPs should take the Euro value recorded at the time the transfer is executed by the originator.

3.5.2 As per Regulation 2A of the Wire Transfer Regulations, and with specific application to the Travel Rule transfers of funds not exceeding EUR 1,000, the VASP does not need to verify the information on the payer unless there are reasonable grounds for suspecting that the funds to be transferred are connected to money laundering or the financing of terrorism.

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

3.5.4 As per UK Guidance[2], the characteristics of the transactions should be 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 three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

3.6 In-scope transfers

3.6.1 Intragroup transfers (those transfers between different legal entities within the same group).

3.6.2 Transfer between VASPs where the originator and beneficiary are the same person (e.g. the same person has accounts with two different VASPs).

3.7 Out-of-scope transfers

[2] JMLSG-Guidance-Part-I June-2023-version, para 5.3.7

3.7.1 Transfers where both the originator and beneficiary hold accounts with the same VASP.

3.7.2 Transfers between two VASPs acting on their own behalf.

3.7.3 Transfers between the same legal entity within the same VASP.

3.7.4 Transfers of funds not exceeding EUR 1,000 unless there are reasonable grounds for suspecting that the funds to be transferred are connected to money laundering or the financing of terrorism.

3.8 Guidance for intermediary VASPs

3.8.1 **Definition**: an intermediary VASP is a VASP that facilitates or participates in the processing of a virtual asset (VA) transfer between an originating and a beneficiary VASP, without having a direct business relationship with either the originator or the beneficiary.

3.8.2 **Example scenarios:**

3.8.3 **First scenario:** where VASP A offers 'safekeeping or administration of virtual assets' to customers, and has a sub-custody contract with VASP B, which initiates and receives virtual asset transfers on behalf of VASP A the Travel Rule applies to both VASPs.

It is expected that VASP A collect and supply VASP B with the required information. It is expected that VASP B ensure that the required information is received from VASP A and then passed on with the transfer to a third party.

Exception: custody for Collective Investment Vehicles

Where a VASP provides safekeeping or administration of virtual assets on behalf of a collective investment vehicle (such as a fund), and the fund is the direct customer of the VASP, the Travel Rule obligations apply in respect of the fund only. The unit holders or investors in the fund are not considered customers for the purposes of the Travel Rule.

Appendix A sets out the expectations where a VASP (typically an exchange) is using a third party custodian to safeguard and transfer client assets on their behalf.

3.8.4 **Second scenario:** VASP A (intermediary VASP) operates an over-the-counter (OTC) trading desk and executes transactions using proprietary funds provided by other VASPs, without acting under instruction from a third party customer. In such cases, where VASP A and its counterparties are each acting on their own behalf, the transaction is out of scope for the Travel Rule. To support this determination, VASP A may rely on formal documentation, such as a service agreement or memorandum of understanding confirming that the counterparty VASP is not acting on behalf of a customer.

Where a customer of VASP A initiates an OTC trade by sending virtual assets from a wallet hosted by VASP B, VASP B is acting on behalf of the customer and is therefore in scope of the Travel Rule. VASP B is expected to transmit the required originator information to VASP A. Following execution, when VASP A settles the traded assets back to the customer via VASP B, VASP A is then acting on behalf of the customer and must transmit the required beneficiary information to VASP B.

3.8.5 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 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 we can understand why the transfer of virtual assets was completed, delayed or refused.

3.8.6 It is expected that the intermediary VASP send on any requested information which is received after it has transferred the virtual asset as soon as is practicable.

3.8.7 It is the responsibility of the VASP to determine if they are acting in the capacity of an intermediary.

4 Jersey VASP to or from non-VASP

4.1 Transfers to or from unhosted wallets

4.1.1 **Definition:** a wallet not hosted by a VASP.

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

4.1.3 When determining the risk rating for an unhosted virtual asset transfer, VASPs may take into account:

4.1.3.1 the purpose and nature of the business relationship with the owner of the unhosted wallet

4.1.3.2 the jurisdiction (if known) of the unhosted wallet

4.1.3.3 the value and frequency of the transfer(s)/linked transfers to/from the unhosted wallet

4.1.3.4 outputs from Blockchain Analytics solutions detailing any association of the unhosted wallet with illicit activities

4.1.4 In higher risk cases, VASPs should also consider further steps to verify the ownership and control of the unhosted wallet.

4.1.5 Where a VASP does not obtain sufficient information to be comfortable with the ownership and control of the unhosted wallet, the transferred virtual assets should not be made available to the intended beneficiary.

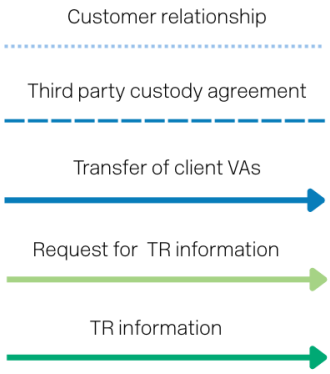
Appendix A – intermediary VASPs

Travel rule expectations for custodian-exchange relationships

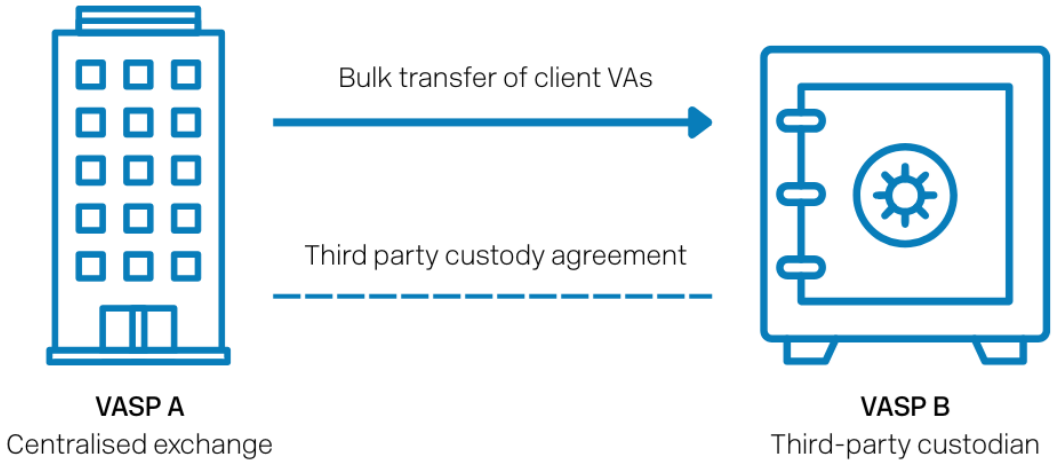
This appendix sets out expectations for Travel Rule compliance in scenarios where a third-party custodian (VASP B) provides services to a centralised exchange (VASP A). These examples are intended to clarify how the Travel Rule applies when virtual asset transfers are processed between VASPs or involve unhosted wallets, particularly in cases where VASP B is acting as an intermediary on behalf of VASP A.

Below we have set out three scenarios, where:

- VASP A = a centralised exchange
- VASP B = a third party custodian
- VASP C = another centralised exchange

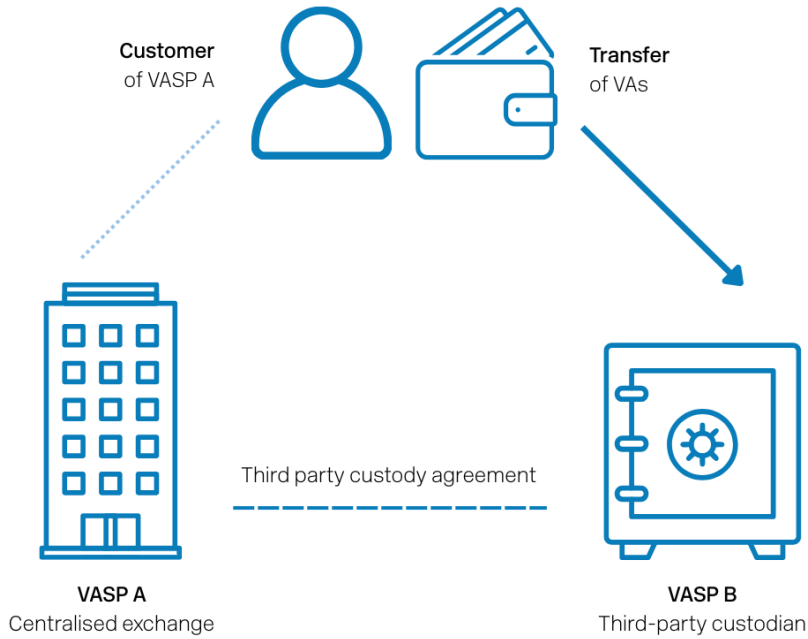


Scenario 1 – VASP A engages VASP B as a third party custodian for client virtual assets
VASP A makes a bulk transfer of client VAs to VASP B
Travel Rule: **Out of scope**. The transfer from VASP A to VASP B is executed by and on-behalf of VASP A.

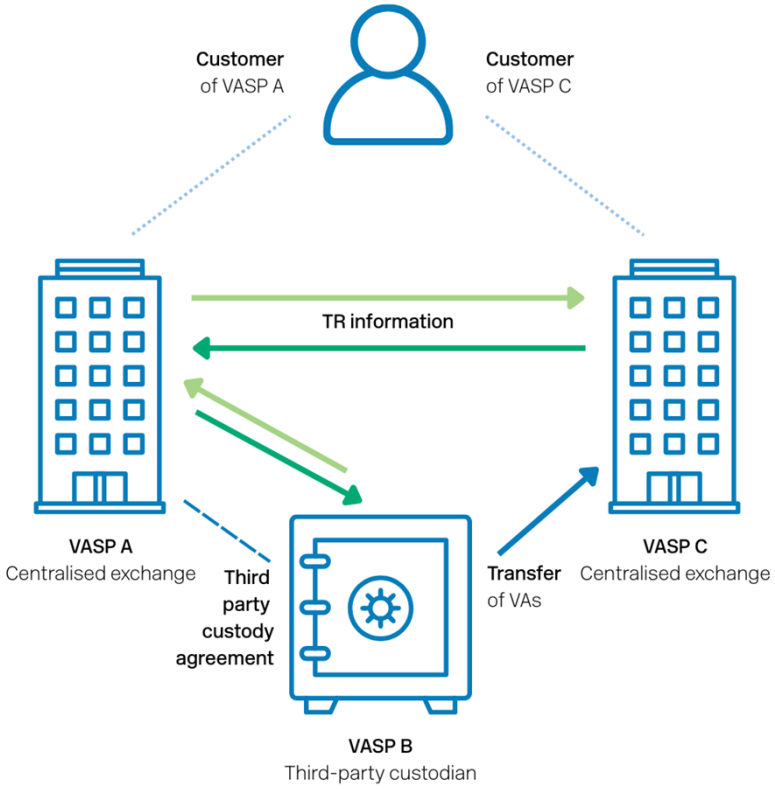


(all below scenarios assume Scenario 1 has already played out i.e. a custody contract is in place)

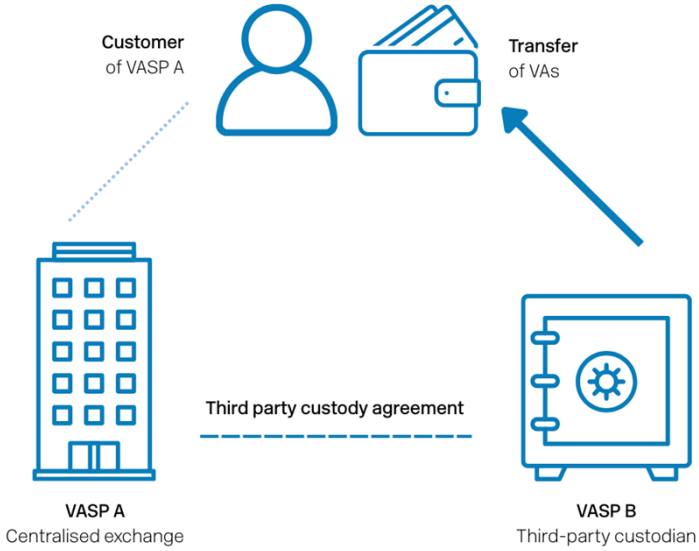
Scenario 2.1 – client of VASP A deposits VA into VASP B from an unhosted wallet*
VASP B receives VAs on behalf of VASP A for an existing client of VASP A from an unhosted wallet.
Travel Rule: **Out of scope**. TR only applies for VASP to VASP transfers.



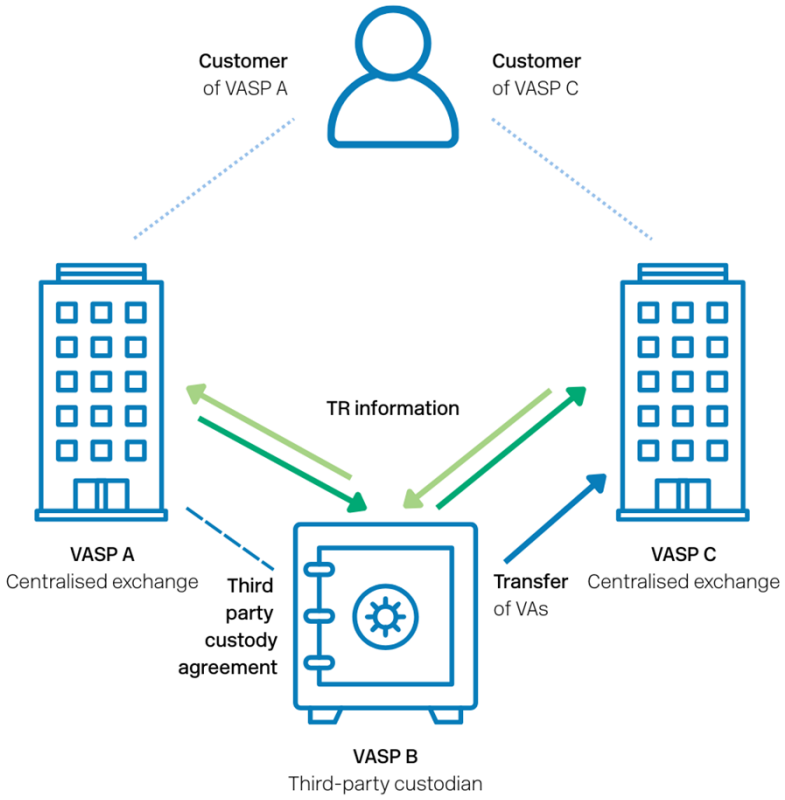
Scenario 2.2 – VASP C processes a client instruction to transfer VA from VASP C to VASP B (custodying on behalf of VASP A)*
A client of both VASP C and VASP A requests a transfer of VAs from their hosted wallet at VASP C to VASP B. VASP B receives the assets on behalf of VASP A
Travel Rule: **In scope**, VASP A must request TR information from VASP C and share that information with VASP B. VASP B is responsible for ensuring it receives the required information from VASP A.



Scenario 3.1 – client of VASP A requests to transfer VAs to unhosted wallet**
VASP B executes transaction on behalf of VASP A. VAs are sent to client's unhosted wallet
Travel Rule: **Out of scope**. TR only applies to VASP to VASP transfers.



Scenario 3.2 – Client of VASP A requests to transfer VAs to hosted wallet (VASP C)**
VASP B executes transaction on behalf of VASP A. VAs are sent to VASP C
Travel Rule: **In Scope**. VASP A must provide the required Travel Rule information to VASP B, which, as the processing intermediary, is responsible for transmitting that information to VASP C.



*In these Scenarios we are assuming that the transfers are being sent directly to the custodian (VASP B)
**In these Scenarios we are assuming the transfers are made direct from VASP B to the recipient