

Travel Rule Course



Introduction to the Travel Rule

Congratulations on beginning the Travel Rule Course from Sumsub! Session highlights accompany every module for your reference.

Module 1 covers the following areas:

- Travel Rule Fundamentals
- Compliant Companies
- Financial Action Task Force (FATF) Travel Rule Requirements
- Jurisdiction-Dependent Specifics
- Risks of Non-compliance

Your hosts:



Ioana Surpateanu,
CSO at Domin Network,
Chair of the Board at
Domin Foundation



Edona Vata,
Co-Founder and
Partner at BitCompli

Session 1

Travel Rule Fundamentals

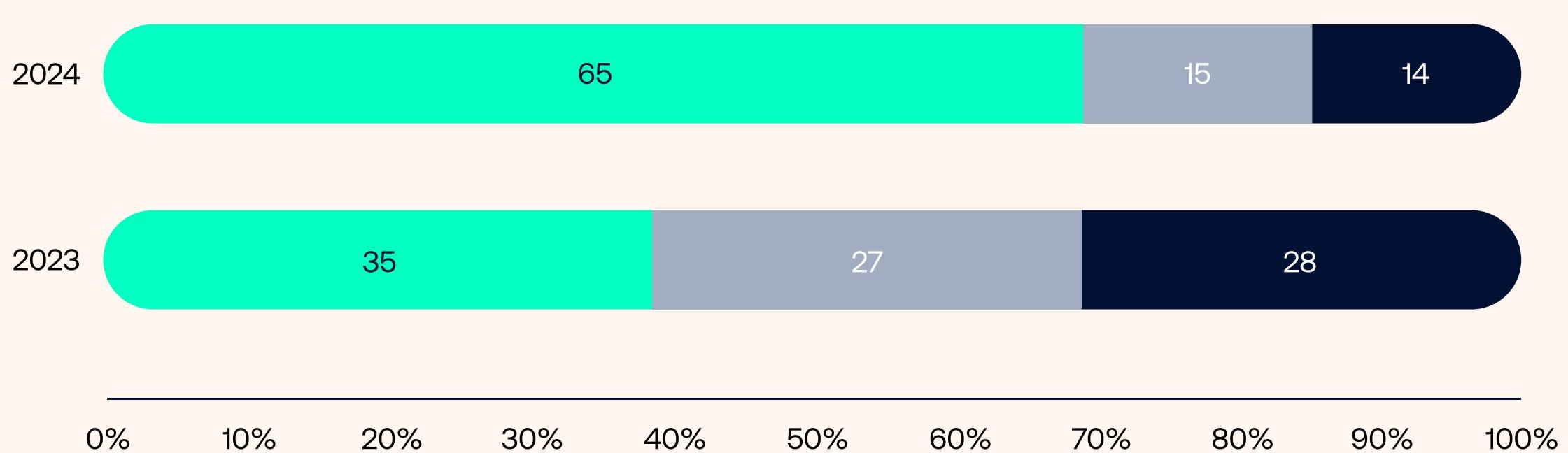
Travel Rule history:

It was conceived in the U.S. in 1996 as part of the Bank Secrecy Act rules issued by [FinCEN](#) to help detect and prevent money laundering. Virtual Asset Service Providers (VASPs) were included later under the Travel Rule to address emerging risks in the crypto sector. Financial institutions, including banks and VASPs, must comply with the Travel Rule by sharing sender and receiver information for transactions above a certain threshold to prevent illicit activities.

The [2024 FATF survey](#) reports that 70% of respondents (65 of 94 jurisdictions, excluding those that prohibit or plan to prohibit VASPs explicitly) have passed legislation implementing the Travel Rule.

Jurisdictional implementation & enforcement of the Travel Rule

- Has passed legislation putting in place the Travel Rule for VASPs
- In the process of passing legislation to put in place the Travel Rule for VASPs
- None of the above



Source: FATF (2024), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs

Session 2

Compliant Companies

Which virtual asset service providers (VASPs) need to comply? You must know this first to determine if you are subject to Travel Rule requirements.



The Financial Action Task Force (FATF) has outlined its full definition of a VASP in its [Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers](#) document.

A VASP is a business that conducts one or more of the following activities or operations for (or on behalf of) another natural or legal person:

- Exchange between virtual assets and fiat currencies
- Exchange between one or more forms of virtual assets
- Transfer of virtual assets
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Other terms for VASPs:

- EU: Crypto service providers
- Singapore: Digital payment token providers
- US: Money services business
- UK: Cryptoasset businesses

Who else is in the scope?

Under certain circumstances, the following services may be considered VASPs:

- DeFi platforms
- VA escrow services
- Brokerage services
- Order-book exchange services
- Advanced trading services
- ATMs

Session 3

Financial Action Task Force (FATF) Travel Rule Requirements

For a VASP to comply with the Travel Rule, it must obtain and record specific information about both the originator and the beneficiary of a transaction:

Information on the Originator:

- **Full Name**
- **Distributed Ledger Address and/or Crypto-Asset Account Number:** If the transfer is registered on a DLT network.
- **Physical Address and Identification:** Including official personal document number, customer identification number, or date and place of birth.
- **Legal Entity Identifier (LEI):** If available, or another official identifier.

Information on the Beneficiary:

- **Full Name**
- **Distributed ledger address and/or crypto-asset account number:** Similar to the originator's details.
- **Legal Entity Identifier (LEI):** If available or relevant.

Travel Rule thresholds:

Thresholds for VASPs mandate sharing customer information for transactions above a specific value. The threshold amounts can be different depending on the jurisdiction.

Travel Rule steps summary:

- 1) Originating VASP: data collection and verification
- 2) Counterparty VASP attribution and due diligence
- 3) TR transaction
- 4) Beneficiary VASP: TR transaction processing

All of the above steps should be completed before the transaction reaches the blockchain.

Identifying wallet types

The type of wallet is verified by analyzing transaction metadata and wallet addresses to determine if they belong to a hosted service or are self-hosted.

Sumsup has partnered with 21 Analytics to enhance its Travel Rule solution, enabling VASPs to verify user ownership of self-hosted wallets. This includes analyzing transaction metadata to ensure compliance so we can accurately identify 500+ wallet types.

Unhosted/self-hosted wallets:

Executing a VA transaction with an unhosted or self-hosted wallet is up to the ordering VASP itself.

There are two possible options:

- 1)** Applying additional risk control measures, such as verifying the identity of the unhosted wallet owner.
- 2)** Choosing to process transactions to VASPs and other obliged entities and/or unhosted wallets that the VASP classes as reliable.

Missing counterparty VASP

If there is no counterparty VASP or other obliged entity, the following actions should be taken:

- Obtain the originator and beneficiary data from its customers directly
- Screen this data and the transaction itself for potential red flags
- Check whether the transfer is within its risk appetite and what additional safeguards could be applied to execute it
- Retain the records about his procedure

Session 4

Jurisdiction-Dependant Specifics

Although the FATF Recommendations are very authoritative, they are not legally binding, which is why countries have a lot of flexibility when implementing them into domestic legislation.

Summary: Differences in jurisdictional approach

- The sunrise issue
- Interacting with unlicensed/unregistered VASPs
- Transactions with unhosted wallets
- Counterparty due diligence
- The de minimis threshold
- Scope of the data to be transferred

The sunrise issue

The term ‘sunrise issue’ relates to the initial phase of imposing Travel Rule regulations on the cryptocurrency world. The metaphor refers to the sun rising at different times in different regions. Some countries have already implemented the Travel Rule, so the sun is ‘up,’ but others have not, so ‘the sun is ‘down.’

Different approaches to CDD requirements in Travel Rule implementation

When implementing the Travel Rule at the national level, jurisdictions have adopted different approaches regarding customer due diligence (CDD) requirements for VASPs. These approaches can be broadly categorized into two types:

1) Jurisdictions requiring CDD before data transfer:

Portugal, Mauritius, EU (under certain conditions): These jurisdictions require VASPs to perform CDD on their counterparties before transferring any data. For instance, Portugal has a specific list of data and procedures for verifying counterparty VASPs, ensuring thorough compliance. The European Union also mandates CDD under its latest regulations, although the specifics can vary depending on the transaction's context.

2) Jurisdictions that do not prescribe specific CDD requirements:

Switzerland and Canada: These countries adopt a more principles-based approach, avoiding strict CDD mandates. Instead, they focus on ensuring that VASPs assess and manage risks appropriately according to general AML/CFT guidelines. This allows more flexibility for VASPs to determine their procedures based on the transaction's risk profile.

Even within countries that require CDD, the extent and specificity of required data can differ significantly. For example:

Portugal specifies a detailed list of data points and verification steps as part of its CDD process.

Mauritius and the British Virgin Islands (BVI), on the other hand, only set a general expectation for due diligence without prescribing exact data requirements.

Session 5

Risks of Non-compliance

Financial penalties: Consequences for non-compliance

Estonia:

Up to 300 units for executives or employees, and/or up to 400,000 euros for legal persons (International Sanctions Act).

Namibia:

Not exceeding N\$10,000,000.

According to the Namibian Virtual Assets Act, “A person who contravenes or fails to comply with the requirements commits an offense and is liable upon conviction to a fine not exceeding N\$10 000 000 or imprisonment for a period not exceeding ten years, or to both such fine and such imprisonment”.

In the UK, the Financial Conduct Authority (FCA) has enforcement powers, which can be applied to individuals and firms that do not meet the regulator’s standard. These powers could include a firm’s authorization withdrawal, prohibition from carrying out regulated activities, suspension, and eventual fines.

Non-compliance with the Travel Rule can result in severe consequences, such as license revocation in jurisdictions like Austria and the UK, where regulators strictly enforce these rules to prevent money laundering and other financial crimes.



End-of-session quiz

Don't forget to take the quiz to test your knowledge!

Further Reading →

