Quick Guide: What Is the Travel Rule?

October 2025

01 What Is the Travel Rule?

In 2019, the Financial Action Task Force **(FATF)** broadened its scope of anti-money laundering and counter-terrorist financing (AML/CFT) measures to cover virtual assets and virtual asset service providers (VASPs), represented in **Recommendation 16**, commonly referred to as the **Travel Rule**.

This expansion aimed to curb criminal and terrorist misuse within the virtual asset sector.

Upon implementation, Rec 16 acts as a regulatory framework that VASPs must adhere to when executing virtual asset transfers.

As outlined in Recommendation 16, VASPs are **mandated to gather, verify, and exchange specific customer information before facilitating any virtual asset transfer.** Additionally, it outlines the protocols governing transactions involving self-hosted wallets.

The FATF's Travel Rule is a significant measure in the ongoing battle against AML/CFT. Its primary objective is to empower VASPs and financial institutions to prevent terrorists, money launderers, and criminals from using wire transfers, including those involving virtual assets, to transfer funds.

Moreover, the Travel Rule aids in the detection and mitigation of such illicit activities, should they occur. Its principal aims ensure the accessibility of originator and beneficiary information for the following purposes:

- Assisting law enforcement authorities in detecting, investigating, prosecuting, and tracing terrorists or other criminals and their assets.
- Facilitating financial intelligence units in the scrutiny of suspicious or unusual transactions.
- Equipping ordering, intermediary, and beneficiary VASPs and financial institutions with the means to identify and report suspicious transactions, freeze funds, and pre-empt transactions involving sanctioned individuals or entities.

02

Which Businesses Are Affected by the Travel Rule?

In 2019, the FATF recommended that the Travel Rule apply to VASPs for both fiat and virtual asset transactions.

It was determined that the Travel Rule is to be implemented if

- The transactions involve a traditional wire transfer or
- A virtual asset transfer between a VASP and another obliged entity or
- A virtual asset transfer between a VASP and a self-hosted wallet.

The latter two points were included in the 2021 FATF's revised guidance on a **Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.**

VASPs are also required to undertake due diligence on their counterparties before transferring any information and trust the counterparty with their customers' data

What Is VASP Counterparty Due Diligence?

Due diligence is the process of conducting a thorough investigation or research into a potential business partner, client, or any other entity with which you intend to establish a business relationship.

The goal is to gather relevant information to assess their credibility, financial stability, legal compliance, and other factors that could impact the business relationship.

In the context of VASPs, this would involve investigating the background and legitimacy of another VASP before establishing any kind of financial or operational connection.

Examples of conducting due diligence are through the collection and storage of identification data, copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.

03 What Information Does the Travel Rule Require?

As per the **FATF Travel Rule**, VASPs must furnish virtual assets transfers with information on their originator and beneficiary.

Travel Rule Data Required

The following information is to be verified by the originator VASP before transacting:

- Originator's name,
- Originator's account number,
- Originator's physical address OR
- Originator's national identity number, or customer identification, or date and place of birth.

With the below information to be verified by the beneficiary VASP before transacting:

- Beneficiary's name,
- Beneficiary's account number.

The verification process is only a piece of the Travel Rule's core. To implement the Travel Rule successfully, this information is to be transmitted to the beneficiary VASP and stored.

Additionally, the information must be available on request to competent authorities upon request and be stored for a minimum of 5 years.

What Is the Travel Rule's Threshold?

The FATF recommends a threshold of EUR/USD 1000, but there are exceptions to this amount.

For example, in Switzerland, where the threshold is 0. For any transaction that surpasses this amount, information will need to be exchanged between the originator – the person sending the virtual assets and the beneficiary - the person receiving the virtual assets.

04

What Is the Travel Rule for Self-hosted Wallets?

The Travel Rule applies to every crypto transaction between VASPs if the Travel Rule is active in at least one of the transacting VASP's jurisdictions.

Moreover, jurisdiction-dependent, the **Travel Rule can apply to transactions between VASPs and self-hosted wallets.**

Self-hosted wallets earn a separate section - **179 and 180** - in the **updated guidance** from the FATF.

For one, self-hosted wallets are considered of higher risk in general. Also, when receiving a deposit from a self-hosted wallet, a VASP must gather the same data as in a VASP-to-VASP transaction. That means that the VASP needs to obtain the originator's information, but that data can be unverified. The beneficiary data should again be acquired from the originator.

Self-hosted wallet requirements vary from jurisdiction to jurisdiction.

I.e. in **Liechtenstein**, enhanced due diligence must be applied when dealing with self-hosted wallets; wallet owners are to provide proof of ownership.

05

How to Comply with the Travel Rule as a Crypto Business?

The Travel Rule requires data to be exchanged between the originator and beneficiary. For a VASP to successfully do so, it needs a **Travel Rule solution.**

What Is a Travel Rule Solution?

A Travel Rule solution is a complete package, like **21 Travel Rule**.

It is software with an existing protocol. Depending on the capabilities of the software, more than one protocol can be utilised.

What Is a Travel Rule Protocol?

A Travel Rule protocol is a set of rules that define how to transmit customer data between Travel Rule solutions. Often, a Travel Rule protocol follows IVMS 101 to ensure a standard format when transmitting this data.

Usually, if a standard format is not adhered to, your counterparty's Travel Rule software will not be able to process the transaction.

Travel Rule Solution Checklist

Does your Travel Rule solution:

- Support low-value transfers under varying jurisdictional thresholds?

  Cover all virtual asset types?

- Use structured formats like ISO 20022 for compliance and screening?
- Securely exchange Travel Rule data before or during the blockchain transaction?
- Allow the selective submission of Travel Rule data based on jurisdiction or counterparty?
- Seek information on counterparty VASPs for required due diligence?
- Request information on a transaction to determine if it involves high-risk or prohibited activities?
- Enable self-hosted wallet verification?
- Support various self-hosted wallets?

06

What are the Challenges to Implementing the Travel Rule?

The Discovery Problem

The Travel Rule requires VASPs to send customer information to their counterparty, as a crypto transfer must be accompanied by personally identifiable information (PII).

However, a standard wallet address contains no information on the VASP that holds it. So, how is a VASP to know where to send the required Travel Rule data - this is the discovery problem.

The Sunrise Issue

While the global implementation of the FATF Travel Rule is on the uptick, there are still jurisdictions that have not converted it into law.

Meaning that some jurisdictions may have the Travel Rule in place, and their counterparties may not.

This becomes an issue as compliant VASPs (in countries where the Travel Rule is active) are required to collect and transmit originator and beneficiary information.

But if the counterparty VASP is in a jurisdiction where the rule is not yet enforced, they might not be able or willing to obtain or receive this data.

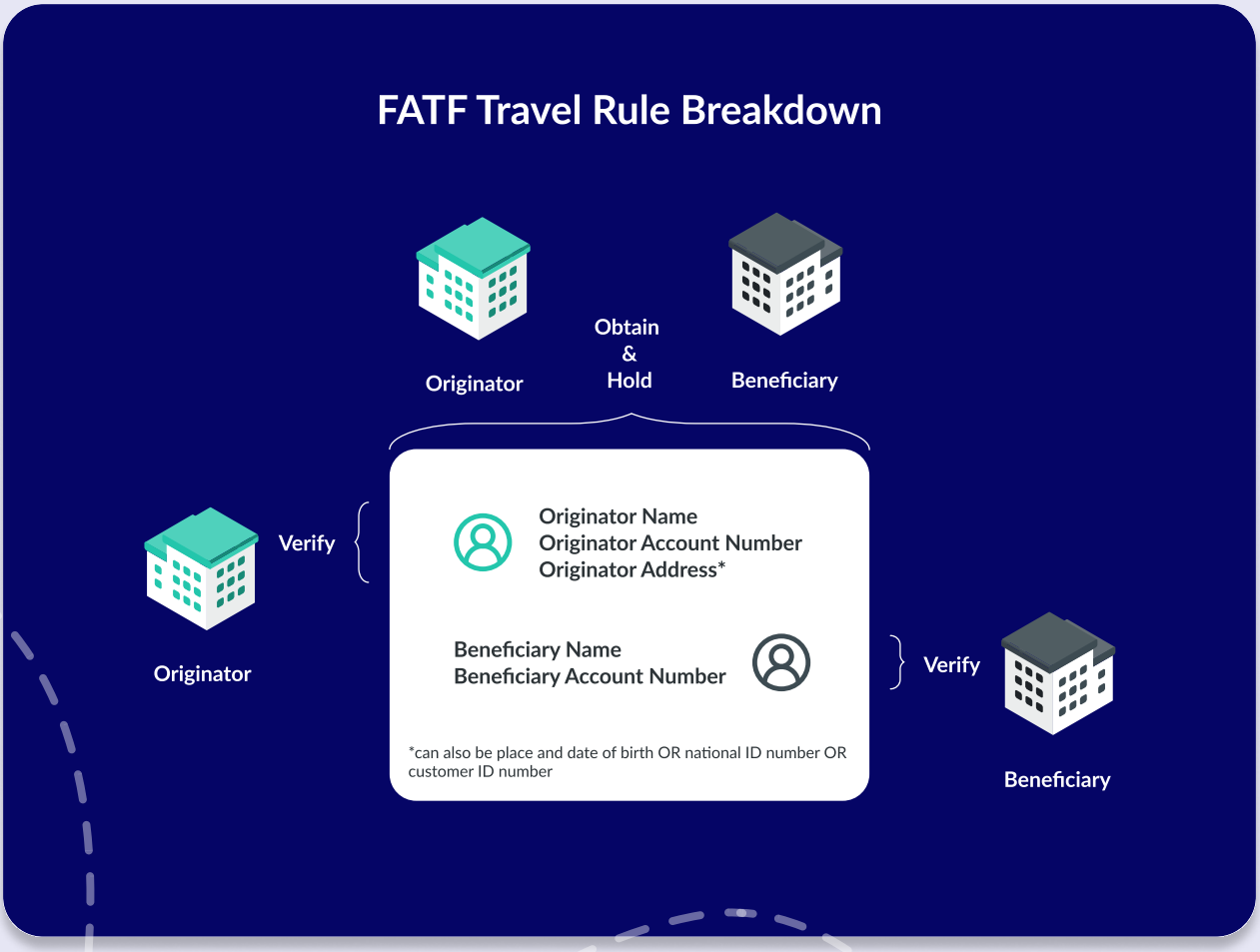
Data Protection

As the Travel Rule mandates the collection, holding, and sharing of delicate customer data, VASPs need to ensure that their solution can do so while conforming to their jurisdiction's data protection laws.

Moreover, VASPs need to consider their counterparty's data protection laws. Perhaps their counterparty's data protection laws are less stringent, or perhaps their counterparty does not have appropriate data protection methods in place.

In circumstances like these, sharing customer data could put both the originator and the customer at risk.

07 Travel Rule Data Breakdown



08

Travel Rule Development & Implementation Timeline

1989

FATF established at G7 summit in Paris.

1990

Report issued Forty Recommendations.
A comprehensive plan to fight money laundering.

2001

The Eight Special Recommendations were issued to deal with terrorist financing.

2012

Reviewed the existing standards and published a revised version.

2014

Started looking at virtual assets.

2015

Published first guidance for RBA to virtual currencies focusing on regulated exchanges.

2018

Adopted changes to recommendations to explicitly clarify that they apply to financial activities involving virtual assets. Definitions added for virtual assets and virtual asset service providers (VASPs).

2019

Published note to Recommendation 15 and RBA guidance for virtual assets and VASPs.

2020

First 12 month review and revised FATF standards on virtual assets and VASPS published.

2021

FATF publishes draft of Updated Guidance clarifying definitions and giving examples.
Second 12 month review and revised FATF standards on virtual assets + VASPS published.
Final version of Updated Guidance published.

Present Day

Ongoing global adoption of the Travel Rule.
The FATF applied updates to Recommendation 16, to be in effect from 2030.

09 Travel Rule FAQs

What Is a VASP?

The FATF defines a VASP as *"any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities (stated below) or operations for or on behalf of another natural or legal person."*

As defined by the FATF, VASP activities include:

- Exchange between virtual assets (crypto 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.

[FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. Page 109]

What Is a Virtual Asset?

The FATF defines a virtual asset as a *"digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes".*

The FATF generally does not consider non-fungible tokens (NFT) as virtual assets, but this depends on their characteristics. They may fall under the definition if they are used for "payment or investment purposes".

Examples of virtual assets include specific currencies like bitcoin and Ether, as well as stablecoins.

10 Travel Rule FAQs

How Long Should a VASP Retain Travel Rule Data?

This varies according to jurisdiction. Usually, VASPs need to retain Travel Rule data for a minimum of 5 years.

The FATF

The FATF's Recommendation 11, page 15, states that customer data (obtained through customer due diligence measures) be retained for five years for record keeping and transaction monitoring. **The FATF Recommendations.**

The European Union

According to the **Final Draft AMLR & 6th AMLD Framework**, Chapter VI Data Protection and Record-Retention, Article 56, the EU requires a period of 5 years. This time frame is reiterated in **DIRECTIVE (EU) 2015/849 Chapter V, Article 40 and point (44)**.

Switzerland

According to **Article 958f of the Swiss Code of Obligations,** data is to be retained for 10 years.

Do Transactions to Self-hosted Wallets Fall under the FATF Travel Rule Regulation?

Nearly every jurisdiction that has implemented the Travel Rule includes self-hosted wallets within its scope.

The FATF Recommendation 16 stipulates that VASPs must still identify the owner of the self-hosted wallet if at least one obliged entity is involved in the transaction.

Depending on local regulations, collecting this information may be sufficient, while in other cases, VASPs must verify the ownership of the self-hosted wallet.

The following jurisdictions include self-hosted wallets in their implementation of the Travel Rule:

- Switzerland
- The EU
- The UK
- Cayman Islands
- Gibraltar
- Hong Kong
- Isle of Man
- Liechtenstein
- Türkiye
- Singapore
- The US

11 Why Choose 21 Analytics

21 Travel Analytics is a leading developer of on-premises Travel Rule solutions.

Apart from meeting the FATF Recommendation 16 requirements, it is most VASPs' go-to solution due to its privacy-respecting nature and self-hosted wallet support options.

Moreover, 21 Travel Rule, 21 Analytics' Travel Rule solution solves the VASP discovery problem with its Travel Address, can be up and running in less than an hour, supports more than 50 blockchains, 520+ wallets and over 2800 digital tokens ensuring Travel Rule compliance.

Request a Demo

Additional Reading

- 21 Travel Rule
- 21 Travel Rule Pricing
- 21 Travel Rule Release Notes
- 21 Travel Rule Product Documentation

21 Analytics AG Zug, Switzerland

info@21analytics.ch
www.21analytics.ch