

Travel Rule Compliance with Sumsub



Table of contents

02/12

1. Decoding the Travel Rule	3
2. Who is affected by the Travel Rule?	4
3. Key requirements	5
4. Which countries enforce the Crypto Travel Rule?	6
5. Travel Rule Implementation Challenges in Crypto	7
6. The solution	9



This white paper explores balance between regulatory compliance and the precision and smoothness of daily cryptocurrency transactions, focusing primarily on the Financial Action Task Force's (FATF) Travel Rule. It discusses the Travel Rule's origins, implications for stakeholders, challenges, potential solutions, and its future in the fast-evolving world of crypto.

The rise of cryptocurrencies has brought an evolution in financial regulations to mitigate the risks associated with the sector. One such measure is the FATF's Recommendation 16: Wire Transfers, also known as the Travel Rule. Initially aimed at traditional financial institutions but now extending to Virtual Asset Service Providers (VASPs), the Travel Rule's primary objective is to increase transparency in transactions, preventing misuse of digital assets for money laundering or terrorist financing.

The key requirements of the Travel Rule for VASPs include the collection, verification and transferring of crypto sender and recipient information, such as personal identification information and wallet addresses, immediately and securely.

Who is affected by the Travel Rule?

04/12

The Travel Rule has broad-reaching implications for an extensive array of entities operating within the cryptocurrency ecosystem. However, VASPs are affected most directly.

According to the FATF, a VASP is a natural or legal person who, as a business, conducts the following activities:

- ✓ 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

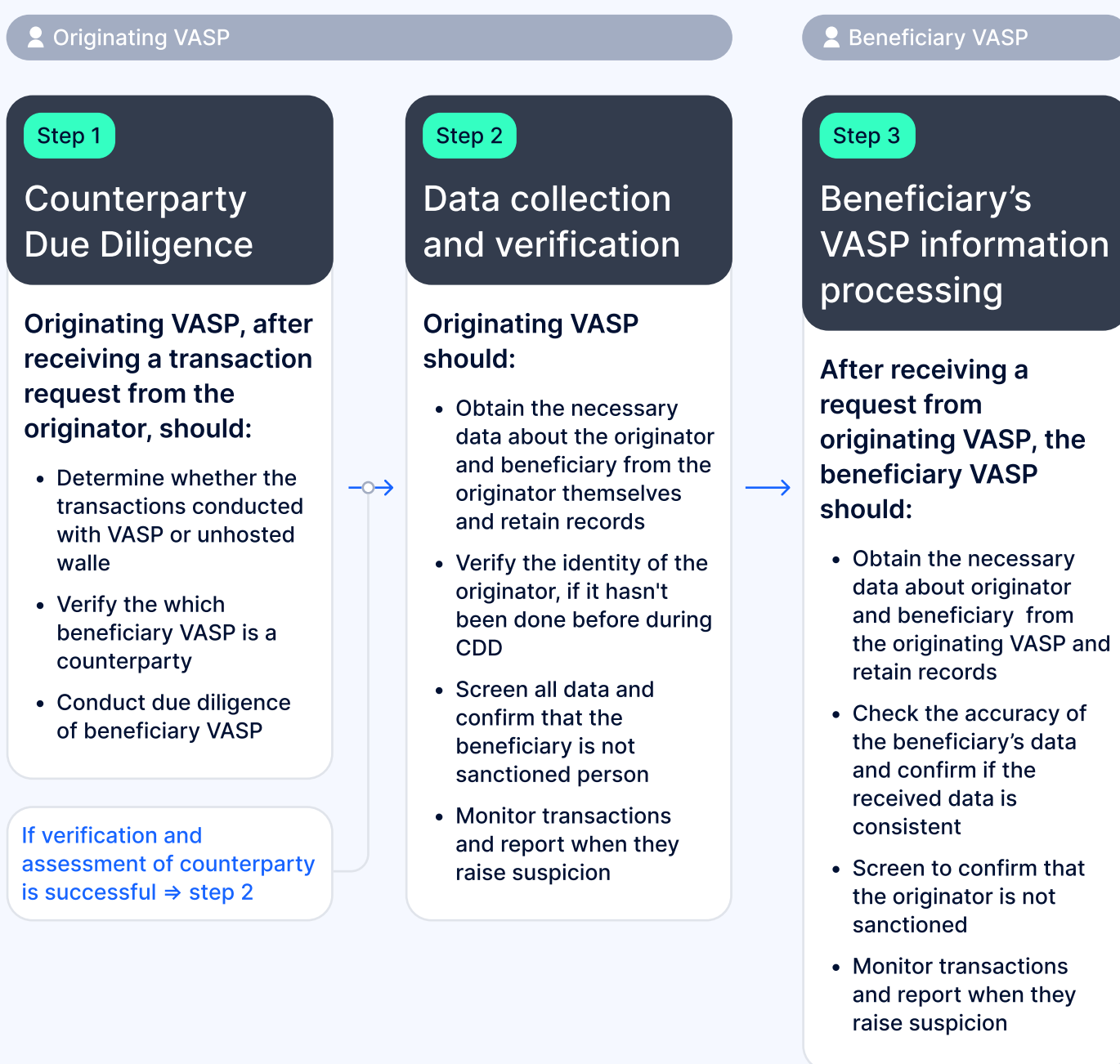
VASPs are now required to implement Travel Rule measures in addition to traditional AML measures such as Know Your Customer (KYC) procedures, ongoing monitoring, sanctions screening, record-keeping and other compliance measures.

Key requirements

05/12

The Travel Rule aims to add traceability to transactions, therefore preventing money laundering and terrorism financing.

The Travel Rule applies to any transfer of funds exceeding a specific value. The FATF recommends that the Travel Rule be applied to any transaction over \$1,000 involving another VASP, but some jurisdictions have different thresholds. According to the FATF, the Travel Rule flow for two VASPs can consist of the following steps.



* These are general requirements based on the FATF's recommendations and may vary depending on the specific regulations of each country.

Which countries enforce the Crypto Travel Rule?

Over 200 jurisdictions around the world have committed to FATF Recommendations through the global network of FSRBs (FATF-Style Regional Bodies) and FATF memberships. However, the implementation process can take years.

For example, in the UK, the Travel Rule comes into effect in September 2023. Still, many other countries—like the US, Canada, Germany, Switzerland, Japan, Singapore, and Hong Kong, etc.—have already implemented the Crypto Travel Rule. Meanwhile, the EU's Regulation on information accompanying transfers of funds and certain crypto-assets is one notable example that will affect crypto transfers in Europe by the end of 2024.



Travel Rule Implementation Challenges in Crypto

07/12



Establishing a compliant verification process

Every transaction must be screened to determine if the Travel Rule applies. This involves the identification of transaction parties, AML screening, data exchange, and reporting to overseeing authorities, which are challenging tasks.



Protecting data

Exchanging Travel Rule data is a sensitive matter. Data exchange covers message exchange protocols between counterparties and VASP identification. Security breaches may result in significant losses, fines from regulators, and reputational damage.



Ensuring Crypto Travel Rule interoperability

There are different messaging protocols — a set of rules for processing, formatting, and exchanging originator and beneficiary information alongside blockchain transactions. Integrating a whole host of protocols to ensure wide coverage is a constant challenge.

Travel Rule Implementation Challenges in Crypto

08/12



Scaling compliantly and efficiently

Without an automated data exchange and verification solution, VASPs are limited to manual approaches that cannot scale at any reasonable capacity. Thus, complying with global Travel Rule requirements can only be done effectively with automation.



Sunrise issue

Countries are implementing their AML/CFT frameworks at different paces. This means that some jurisdictions require their VASPs to comply with the Travel Rule while others don't—a problem referred to as the “sunrise issue”.



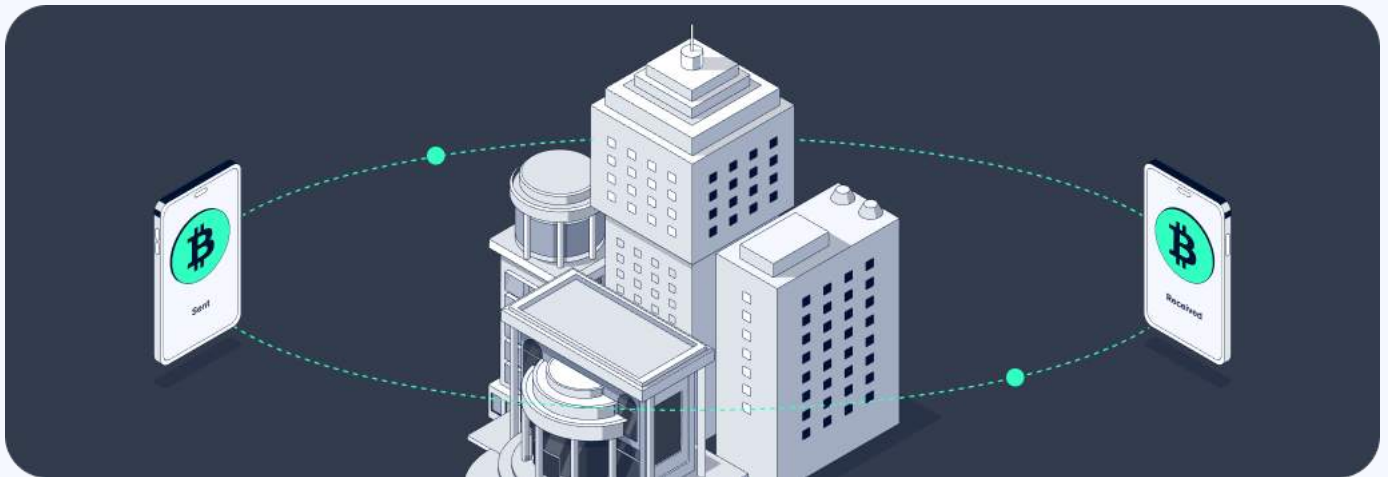
VASP Due Diligence

According to FATF reports, VASP Due Diligence is one of the biggest challenges for crypto companies. The process involves verifying the counterparty VASP before the originating VASP transmits the information required under the Travel Rule. In some cases, VASPs have challenges identifying licensed/registered VASPs. This can result from both a lack of public information on licensed or registered VASPs (e.g., through a database or public register of licensed/registered VASPs) as well as the design of some Travel Rule compliance tools—which, for instance, can only identify counterparties that are subscribers to that particular tool.

The solution

09/12

With Sumsub's Travel Rule solution, your crypto platform can fully automate data exchanges and ensure compliance with regulations worldwide. Engage with 500+ VASPs in our expansive Travel Rule ecosystem.



Automate Travel Rule compliance tasks

Stay ahead by discerning between transactions involving VASPs and unhosted wallets. Be sure that sender and recipient data is meticulously checked and stored transparently for comprehensive monitoring and reporting. Meanwhile, you can monitor transactions with Sumsub's Transaction Monitoring solution and set up different rules, including amount and periods, with corresponding alerts.

Conduct AML and sanction screening

Sumsub provides AML and sanction screening services which check whether a crypto sender and a recipient is present on any global sanctions lists (OFAC, UN, HMT, EU, DFT etc.), watchlists, or adverse media. Sumsub screening covers countries based on ISO 3166 and provides data from a database containing approximately 10,000 independent and reliable data sources from 200+ countries and territories.

Securely exchange sender and recipient data

Rest easy knowing that both originator and beneficiary data is shielded against potential breaches. All data, including that processed in line with the IVMS 101 messaging standard, is encrypted using top-tier methods. Sumsub has a user verification track record that dates back to 2015, and we prioritise data protection.



Our commitment is further bolstered by compliance with EU General Data Protection Regulation (GDPR) and UK GDPR standards and other applicable regulations. Sumsub actively pursues independent audits and certifications pertaining to information security, and data protection.

Introduce interoperability protocols

Sumsub is a protocol-agnostic Travel Rule solution, integrating the IVMS 101 messaging standard for consistent and coherent data exchange. Our platform boasts full interoperability, effortlessly accommodating third-party protocols. This ensures seamless and compliant transactions with partners on a global scale. Moreover, Sumsub goes the extra mile by facilitating an internal protocol for our clients, enabling smooth connections to over 500 VASPs without a hitch.

Delegate VASP Due Diligence to Sumsub

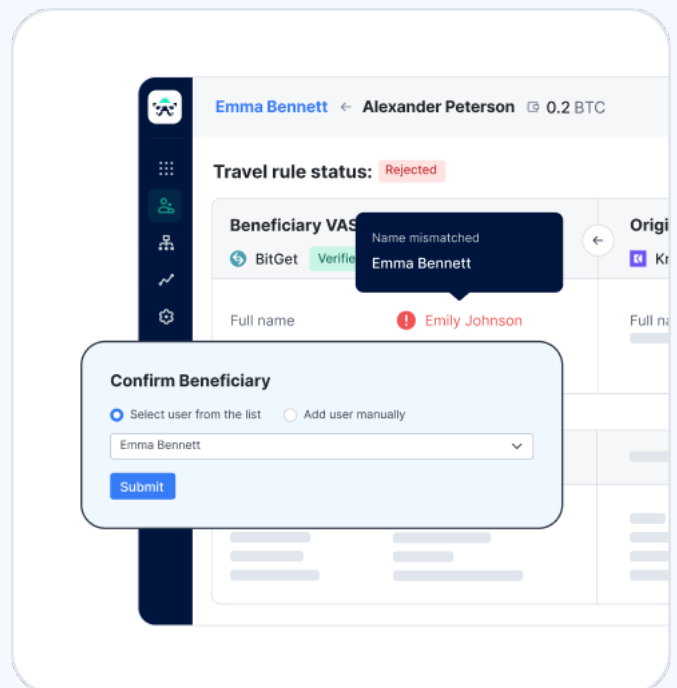
Due Diligence for VASPs is free for Sumsub clients. We know the challenges you may face with the Travel Rule, and our goal is to make the process seamless and hassle-free for you.

Effortlessly reach counterparties

It can sometimes be difficult or impossible to contact a counterparty VASP to execute Travel Rule data transfers. In such cases (particularly when Sumsub clients are an originating VASP) Sumsub has a solution in place.

Take advantage of a Travel Rule solution built for growth

Manual processing can hinder growth. With our platform, enjoy instant transaction processing, automatic verification, and seamless communication between VASPs and regulators. Embrace a Travel Rule solution designed for scalability.



Turn the Crypto Travel Rule into a growth asset with Sumsub

 Originator (Alice)

Transaction

 Beneficiary (Bob)

 Originator's VASP A

Travel Rule information transfer

 Beneficiary VASP B

Actions required

Verify VASP B

Collect and verify info on Alice:

1. Name
2. Wallet address
3. One of:
 - Physical address, or
 - National ID number, or
 - Customer ID number, or
 - Date + place of birth

Collect info on Bob:

1. First name
2. Last name
3. Date of birth
4. Wallet address

Conduct an AML screening on Bob

Monitor transactions



Actions required

Verify VASP A

Obtain data about Alice and Bob from VASP A

Check the accuracy of the info about Bob and confirm if the data is consistent

Conduct an AML screening on Alice

Monitor transactions

[Get a free demo](#) →

