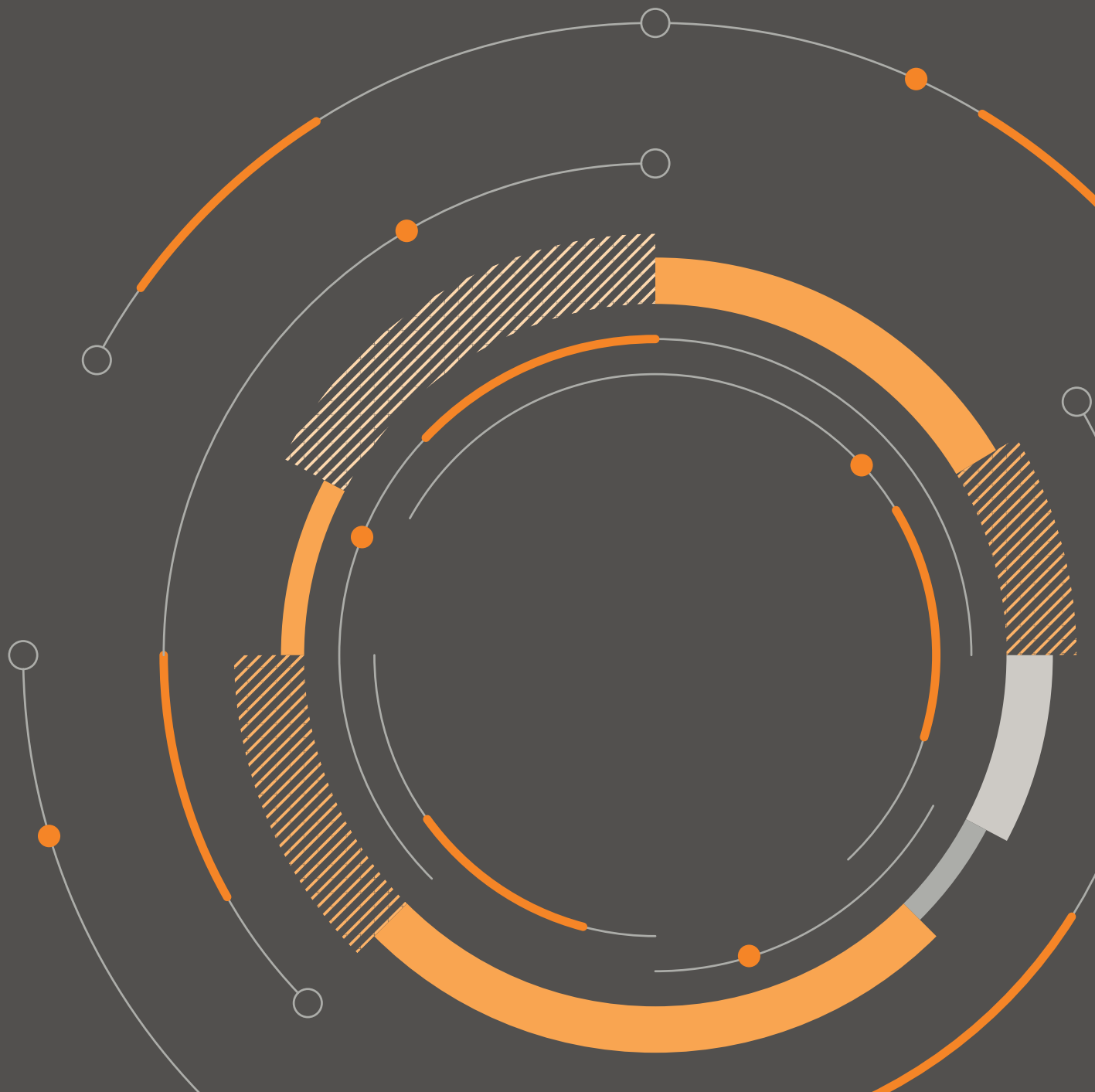
CIPHERTRACE

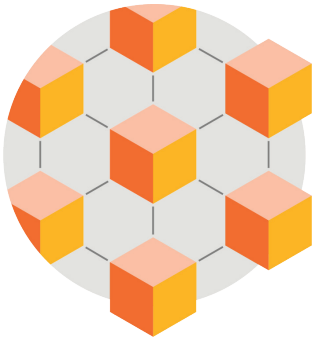
Your go-to guide to the FATF's crypto Travel Rule

GUIDELINES

OCTOBER 2022



Introduction



In the more than three years since the Financial Action Task Force (FATF), a global anti-money laundering watchdog, established the Travel Rule, the guideline has proven to be one of the most significant and complex facets of the cryptocurrency industry for Virtual Asset Service Providers (VASPs). Designed to thwart terrorist financing and other illegal activity, the FATF Travel Rule requires VASPs – such as exchanges, banks, OTC desks, hosted wallets and other financial institutions – to share identifying information about the recipients and receivers of all crypto transactions over a certain threshold.

This requirement has come with a host of challenges for VASPs, such as finding the safest way to collect and share user data, without exposing it to hackers, tyrants, or data brokers. Pressure is now on individual platforms to ensure that the VASP on the other end is legitimate and not out to steal someone's personal information.

To complicate matters even further, it's up to each of the FATF member nations and the broader network of FATF-Style Regional Bodies (FSRBs) and their respective members to decide for themselves how to enforce the Travel Rule – or whether to implement it at all. As a result, regulations vary depending on the country. Different jurisdictions are in different stages of passing the Travel Regulations, in each case for compliance purposes.

To help clarify these complex issues, we've put together this condensed guide to Travel Rule protocol for VASPs (or anyone else interested, for that matter!).

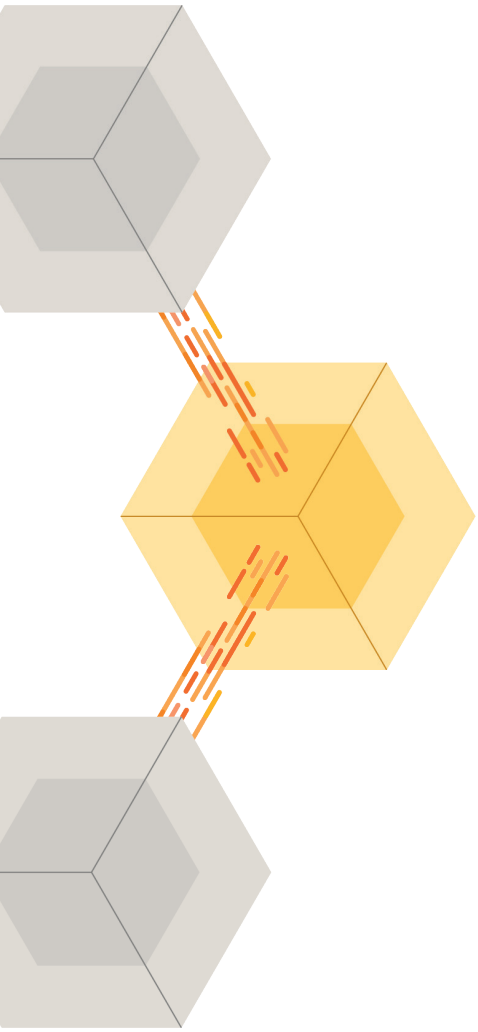
FATF crypto guidance

	BSA	FATF
Threshold	USD 3,0000	USD/EUR 1,000
Name	Required	Required
Account number	When available	Required
Address	Required	Required*
Identity of financial institution	Required	Not required
Transmittal amount	Required	Not required
Execution date	Required	Not required

Recipient information

Name	When available	Required
Address	When available	Not required
Identity of financial institution	Required	Not required
Account number	When available	Required
Any other specific identifier of the recipient	When available	Not required

*Address can be substituted for national identity number, or customer identification number, or date and place of birth



Why the Travel Rule matters

The intent behind the Travel Rule is that sharing information* will allow participants to:

- Block terrorist financing
- Stop payments to sanctioned individuals, entities, and countries
- Enable law enforcement to subpoena transaction details
- Support reporting of suspicious activities
- Prevent money laundering of crypto assets

Risks to individual privacy, and to individuals, in the context of the Travel Rule include:

- Hacks and PII data leaks
- Fake VASPs that attempt to collect PII
- Harvesting, data mining, and selling of user PII
- Monitoring by oppressive regimes, leaks, hacks, data mining, poor security, data brokering
- Distributed denial-of-service attacks and market manipulation

Each VASP must retain the PII it collects, but it does not have to be viewed by the receiving party; nor should it be stored in clear text.

Emerging challenges for Travel Rule compliance

VASPs face strategic and operational risks when implementing the Travel Rule. To mitigate these risks, VASPs should:

- Understand the 'sunrise issue' – staggered enforcement of crypto AML regulations
- Learn how blockchain analytic tools can be used in Travel Rule compliance
- Identify counterparty VASPs and determine whether they are registered
- Undertake counterparty VASP due diligence
- Address cybersecurity, privacy and data protection

*Sharing sensitive financial transactions and personal identifiable information (PII) with unknown or untrusted VASPs creates numerous privacy issues for virtual asset users.

Originator and beneficiary information should include the following:

1. Name and account number of the originator
2. Originator's (physical) address, or national identity number, or customer identification number, or date and place of birth
3. Name and account number of the beneficiary
4. Cross-border transfers below the USD/EUR 1,000 threshold should also include the names and account numbers of originator and beneficiary. However, this information does not need to be verified for accuracy unless there is a suspicion of money laundering or terrorist financing.

History of the crypto Travel Rule

In guidance released on June 21, 2019, the FATF updated recommendation 16 to mitigate the risks of money laundering and terrorist financing associated with virtual asset activities.

Recommendation 16 will require VASPs in member countries to pass customer information to each other when transferring crypto assets. This is similar to the standard that US banks are required to abide by for wire transfers under the Bank Secrecy Act (BSA), which is often referred to as the "Travel Rule."

Travel Rule solutions

The interoperability of solutions is vital to ensuring comprehensive coverage when facilitating crypto transactions with VASPs. Many in the community agree that a solution should use an open-source architecture and be decentralized, secure, scalable, reliable, interoperable and globally available. In addition, CipherTrace believes that a system should also be customizable to fit each VASP's unique wants or needs.

Currently, there are open-source Travel Rule solutions on the market, such as the Travel Rule Information Sharing Architecture (TRISA), as well as enterprise solutions such as CipherTrace Traveler built using TRISA to enhance its capabilities.

Peer-to-peer information exchange

Secure information exchange with any VASP

Verification of destination

Sunrise support

CipherTrace Traveler

CipherTrace Traveler helps financial organizations and crypto exchanges comply with global Travel Rule regulations and FATF recommendations.

Traveler provides the most secure, reliable way to exchange required Travel Rule originator/beneficiary information, even with VASPs that do not currently have a Travel Rule solution. It is fast, easy to implement, and compatible with global messaging standards including IVMS and X.509. Additionally, we have taken steps to ensure that our products, including Traveler, comply with the GDPR and other applicable privacy and data protection laws.

Cryptocurrency Travel Rule regulations by country

Canada

The Financial Transactions and Reports Analysis Center of Canada (FINTRAC), Canada's financial intelligence unit, is responsible for its Travel Rule regulations. The transfer, exchange, or remittance of virtual currency equivalent to $1,000 CAD or more will trigger Know Your Customer (KYC) verification requirements. Canadian VASPs have been expected to comply with Travel Rule guidance since June 1, 2021.

Estonia

In 2017, Estonia became the first jurisdiction to issue crypto licenses. It has now granted upwards of 4,000 of these licenses. Estonia's Financial Intelligence Unit (FIU) passed Travel Rule compliance regulations on March 15, 2022, and enforcement began on June 15, 2022. Estonia has no minimum threshold requirement for compliance with the Travel Rule.

Japan

The Japan Virtual Currency Exchange Association (JVCEA), responding to a March 2021 request from Japan's Financial Services Agency (FSA), has introduced self-regulatory requirements in connection with the Travel Rule. During the transitional period between April 2022 and Oct 1, 2022, Travel Rule obligations apply only if:

- The originator customer is also the beneficiary of the transaction
- The beneficiary VASP is Japanese
- The asset being transferred is ETH or BTC
- The transaction is above ¥100,000

JVCEA's rules do not specify a minimum transaction amount that will trigger Travel Rule obligations after the transitional period

Singapore
On December 5, 2019, the Monetary Authority of Singapore (MAS) published an amendment to the Payment Services Act (PSA), which brought VASPs into the same regulatory fold as other payment service providers. As a result, crypto transactions of S$1,500 or less fall under Travel Rule regulations in Singapore, although only minimal information must be shared. For transactions over S$1,500, VASPS are required to exchange additional PII.

Switzerland
The Swiss Financial Market Supervisory Authority (FINMA) introduced Travel Rule guidance for cryptocurrency on August 26, 2019. The guidance requires that after January 1, 2020, VASPs adhere to Switzerland's existing Anti-Money Laundering Ordinance and its Counter Terrorist Financing (CTF) legislation.

VASPS must comply with the Travel Rule in transactions above $1,000 that involve other VASPs.

In addition, Swiss VASPs should not conduct transactions with unhosted wallets unless the sender can verify that they own the wallet. Transfers to or from a third party's external wallet are possible only if "the supervised institution has first verified the identity of the third party, established the identity of the beneficial owner and proven the third party's ownership of the external wallet."

United Kingdom
VASPs are expected to comply with the Travel Rule beginning sometime around September 2023, 12 months after amendments to the Money Laundering Regulations (MLRs) take effect. VASPs are required to exchange more information for transactions over €1,000 than for transactions below that threshold.

United States
An amendment to the Bank Secrecy Act (BSA) in 2012 expanded the Funds Travel Rule for fiat money to include electronic funds transfers. The Financial Crimes Enforcement Network (FinCEN), a bureau of the Department of the Treasury that is charged with enforcing BSA rules, released guidance in May 2019 stating that the Department would classify cryptocurrency exchanges as money service businesses (MSBs).

As a result, exchanges that operate within the US must now comply with the BSA Travel Rule: For every transfer of $3,000 or more, financial institutions must share the sender's and receiver's KYC data.

Travel Rule standards and protocols

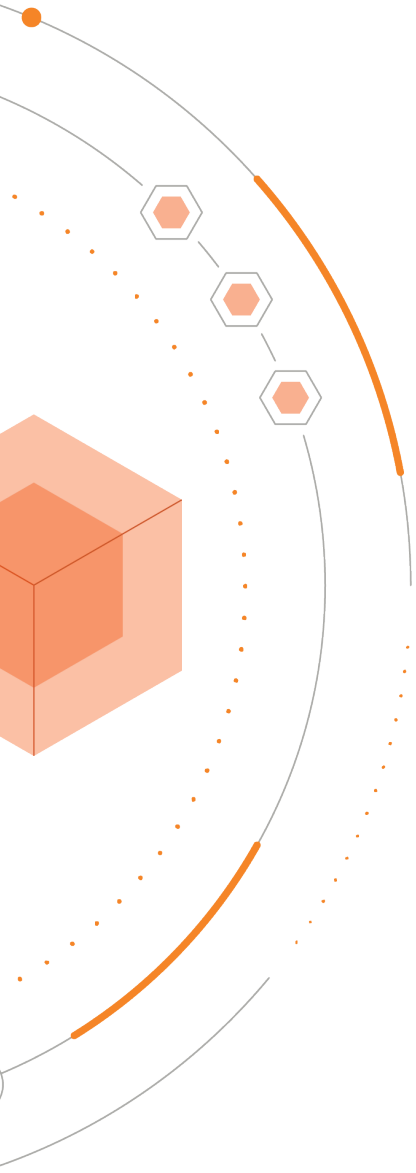
IVMS: The interVASP Messaging Standard (IVMS 101) is the industry standard for exchanging Travel Rule information. It establishes a universal common language for the communication of required originator and beneficiary information between VASPs.

TRISA: The Travel Rule Information Sharing Architecture, developed by the Travel Rule Information Sharing Alliance and sponsored by CipherTrace, is built upon security and cryptography technologies that have been proven for years to secure banking, ecommerce, and government communications. TRISA applies trusted public key infrastructure (PKI) to mutually authenticate VASPs and securely transmit sensitive transaction data.

TRP: The Travel Rule Protocol (TRP) is an API compliance solution. Developed by the ING Group, TRP takes a cue from the fiat-based SWIFT network, creating a similar verification system by using publicly available information, such as a VASP's Legal Entity Identifier (LEI) and public key information, to determine the identities of blockchain addresses. In late 2021 the TRP working group merged with the OpenVASP association.

OpenVASP: An open-source, decentralized common protocol designed for varied implementations across the blockchain environment, the OpenVASP protocol uses a communication handshake protocol that relies on structured messages and session keys to ensure encryption of the transferred information. Relying on Ethereum's decentralized public key infrastructure, VASPs initiate a standardized smart contract to identify themselves on the blockchain. The last 32 bits of the address denote the VASP code. This unique blockchain identity is used in the initial handshake to establish contact with another VASP, as well as in subsequent messaging sessions.

PayString: A universal payment identifier, PayString supports cross-platform communication by using a straightforward and human-readable identifier for each user when transacting currency digitally. The free, open-source code bridges the gap between different users, institutions and currencies (both fiat and crypto), allowing users to transact across a global payment network.



Technology for Travel Rule compliance

X.509 certificates are a global standard for security protocols and the basis for HTTPS – the secure protocol for safely browsing the web. Certificates based on X.509 standards represent the digital identity of a signatory. Some of the Travel Rule protocols use the X.509 certificate to establish communication channels.

A validated X.509 certificate from a certificate authority protects communications between two VASPs by encrypting the connection between them. If a VASP wants more capabilities than are provided in the code – for example, the ability to accept self-certifications – then they are free to do that if they know and trust the VASP on other side. The software is completely customizable to a VASP's specific needs.

Conclusion

Complying with the Travel Rule demands that VASPs come to grips with this complex new regulatory and technological landscape. To protect users' assets and personal information, VASPS must detect VASP-to-VASP payments and ensure that sensitive transaction data is shared only with other Travel Rule-compliant institutions – while also checking for sanctions violations and money-laundering red flags. These requirements call for reliable, interoperable authentication and encryption technology – advanced solutions that can help VASPs make certain that every transaction is seamless and safe.

We're always here to assist. If you have questions or want to find out more about Traveler, get in touch at www.ciphertrace.com

Designed by Mastercard Creative Studio