coinfirm

Complying with FATF Recommendations for Virtual Assets

Travel Rule

Report

September 2020

Cryptocurrency and digital asset transactions necessitate proper oversight and compliance. The prevention of money laundering, terrorism financing, bribery and corruption, tax evasion, and sanctions breaches lies at the centre of this growing area of scrutiny.

In June 2019, the Financial Action Task Force (FATF) updated Recommendation 16, known as the *Travel Rule*. It requires Virtual Asset Service Providers (VASPs) to transmit identifying data, such as names and wallet addresses, for counterparties in a cryptocurrency transaction. These details must remain transparent and allow screening to detect financial crime risks.

A new report developed by Coinfirm, entitled *Complying with FATF Recommendations for Virtual Assets — Travel Rule*, discusses compliance, data protection, technical implementation, and regulatory oversight aspects of the Travel Rule.

We created this report with the support of HM Government of Gibraltar, an expert working group (see below), and with the participation of key crypto exchanges and industry players.

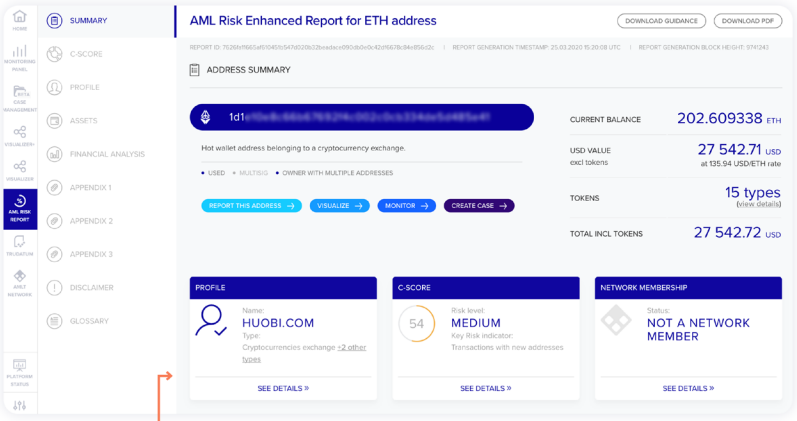
Travel Rule Overview

The Travel Rule emphasises three core principles: focus on outcomes and effectiveness, technological neutrality, and a level playing field for VASPs across all jurisdictions globally. VASPs include providers of custodial digital wallet services, transfer services, and brokerage or investment-related services.

However, we find that a significant slice of the cryptocurrency market consists of peer-to-peer transactions conducted on an *unhosted wallet*. While such transactions are outside of the current scope of the Travel Rule, we recommend the consideration of such unhosted activity moving forward.

Before any virtual asset (VA) transfer takes place, per the Travel Rule, VASPs must perform proper client identification via Know Your Customer (KYC) / Customer Due Diligence (CDD), in line with all locally applicable requirements of the country of licensing or operations. VASPs must obtain, transmit, and retain the required Originator, Intermediary, and Beneficiary information in order to identify and report suspicious transactions. Finally, VASPs should take a Risk-Based Approach to support proportionate responses to managing financial crime risks, focusing time and resources on the highest risk activities.

Jurisdiction-level supervisory controls called for by the Travel Rule include an obligation that VASPs be licensed or registered; that they be subject to supervision and monitoring by competent national authorities; and that national authorities implement penalties, sanctions, and other enforcement measures when service providers fail to comply with their obligations



Report showing counterparty **AML** risk analysis

Extending the Definition of VASPs

The FATF considers a VASP to be any natural or legal person operating as a business and conducting one or more of the following activities for or on behalf of another natural or legal person:

- exchange of value between virtual and fiat forms;
- exchange of value between forms of VAs;
- transfer of VAs;
- safekeeping and administration of VAs or instruments that enable control over VAs; and
- participation or provision of financial services related to the offer or sale of a VA.

The Coinfirm report identifies several gaps and unanswered questions in this seemingly straightforward definition. The “transfer” of VAs entails conducting a transaction on behalf of a counterparty by moving a VA from one VA address or account to another. As such, the definition of a VASP also includes VA transfer services, as well as some VA wallet providers. It includes businesses such as those that host wallets or maintain custody or control over another natural or legal person’s VAs, wallets, or private keys; providers of financial services relating to the issuance, offer, or sale of a VA (such as in an ICO); VA escrow services, including services involving smart contract technology that VA buyers use to send or transfer fiat currency in exchange for VAs when the entity providing the services has custody over the funds; peer-to-peer trading platforms; and other possible business models involving VAs.

Exchange or transfer services may also occur through *Decentralized (or Distributed) Applications (DApps).* In the FATF Guidelines, DApps encompass software programs that operate on a peer-to-peer network of computers running a blockchain platform and allowing the development of secondary blockchains that are not controlled by a single person or group of persons.

FATF Recommendations are clear that the intention is not to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications used for financial activity or conduct as a business. The test of whether any form of decentralised platform or DApp falls within the definition of a VASP in the context of providing ‘exchange’ ‘transfer’ or ‘administration’ facilities is currently complex and subject to interpretation.

The Coinfirm report calls for additional guidance to emerge on more specific criteria that would bring DApp activity within the scope of the definition of a VASP when warranted. However, even in that case, it may be challenging to identify an obliged entity that could be licensed or registered and regulated.

Implementation

According to Coinfirm, six guiding principles should form the cornerstones of any technical solution developed for Travel Rule compliance:

- limiting the amount and use of personal information
- obtaining counterparties' consent
- local regulatory compliance
- common standards for data and messaging
- openness to transactions with non-VASPs
- clear consensus on what constitutes a transaction.

Consistent with the FATF's technology-neutral approach, the required information need not be communicated as part of (or incorporated into) the transfer on the blockchain itself or on another distributed ledger platform. In fact, incorporating and locking personal data into a publicly available and immutable ledger would create several data protection and GDPR issues.

As that VASPs and other obliged entities in VA transfers implement or utilise technical solutions, Coinfirm recommends leveraging commercially available technology to comply, including public and private keys, Transport Layer Security/Secure Sockets Layer (TLS/SSL) connections, and API access. While requirements and data formats should be standardized, solutions should be interoperable rather than coalescing into one single, global solution.

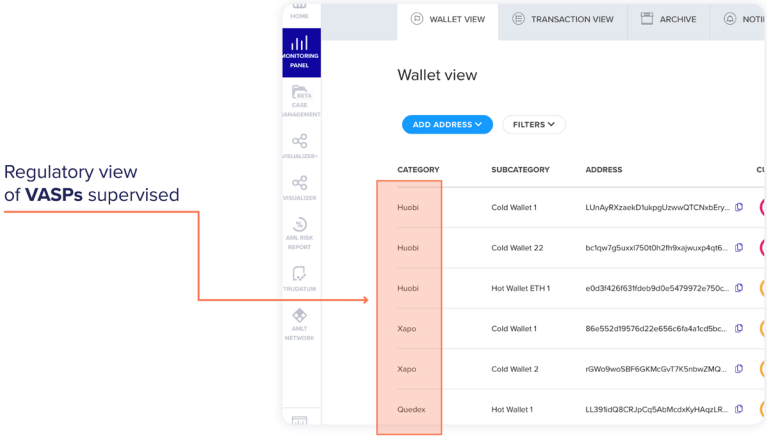
Data Management and Privacy

In managing counterparty and transaction-level data, Coinfirm highlights that certain jurisdictions around the world have implemented regulatory requirements to ensure the data privacy of individuals. Customer identification information will invariably constitute 'personal data' under the terms of the European Union's GDPR, for example. VASPs and other obliged entities must provide customers with clear and transparent information about how their personal data is being used, by whom, and for what purposes. VASPs must also be able to demonstrate that customers have consented to the processing of their personal data in order to meet GDPR requirements.

The report argues that prudent application of *need to know* principles and the adoption of *minimum data required* techniques will assist VASPs and obliged entities in their compliance with general data protection principles across jurisdictions, be they GDPR or other emerging regulations.

Compliance

To ensure that VASPs implement and observe regulations, local regulators must have the ability to carry out appropriate supervision in order to license VASPs as obliged entities and perform oversight of their activities effectively.



To that end, regulators must hold VASPs to seven core oversight and control mechanisms:

1. making required information available to appropriate authorities upon request;
2. where applicable, freezing transactions as well as blocking and prohibiting transactions with designated persons in line with existing regulatory requirements;
3. managing and mitigating the risks of activities that involve the use of anonymity-enhancing technologies or mechanisms, such as AECs, mixers, tumblers, and other technologies that obfuscate the identity of the sender, recipient, holder, or beneficial owner of a VA;
4. having the ability to flag any unusual or suspicious activity for further analysis in a timely manner;

5 prompt reporting of suspicious funds or transactions in the manner specified by competent regulatory authorities;

6 maintaining and screening against a list of “blacklisted” wallet addresses subject to the laws of the VASP’s jurisdiction; and

7 preparing and delivering full audit trails for transactions.

Potential Solution

Sophisticated blockchain analytics solutions that enable risk monitoring and management of addresses and transactions can help VASPs properly manage the underlying Anti-Money Laundering (AML) activity by VASPs. They can also give regulators direct access to audit trails for examining and verifying compliance with Travel Rule standards.

To fully comply with the FATF Travel Rule, two channels need to be created: a P2P network that allows VASPs to exchange and verify required information and a separate blockchain-based system for registering *fingerprints* of transferred data containers.

The recommendation in *Complying with FATF Recommendations for Virtual Assets — Travel Rule* for a solution is as follows:

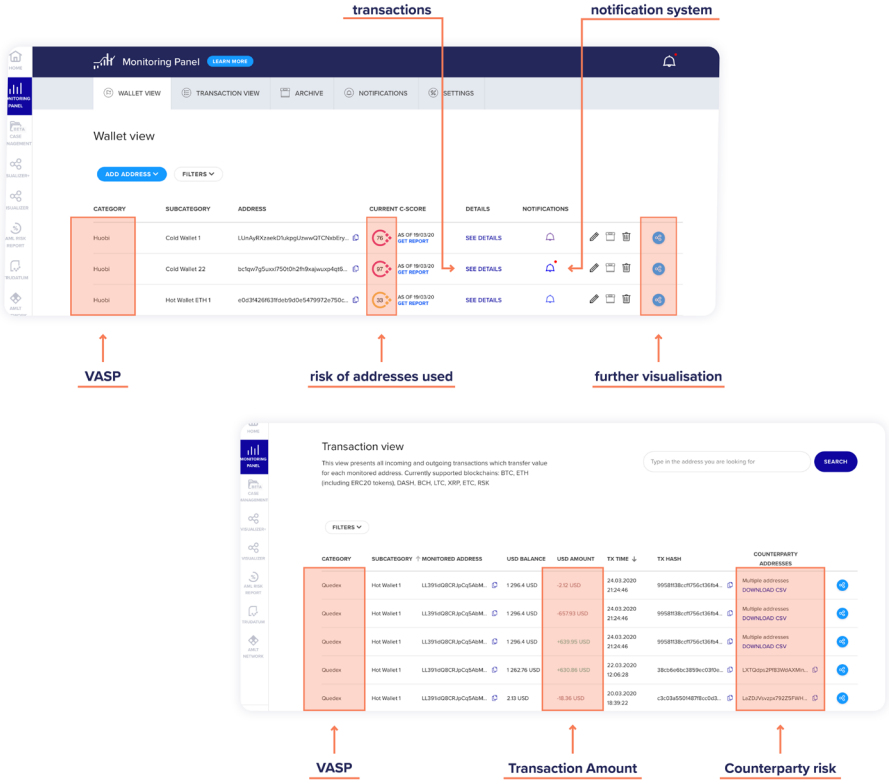
1 Travel Rule SDK Integration – A VASP deploys Coinfirm’s FATF Development Kit on its premises and systems to connect to the Coinfirm FATF Network. It also provides its blockchain addresses and the signatures created with the use of private keys matching these addresses. These are shared among Coinfirm FATF Network nodes. With this in place, the Originator of a transaction commissions the withdrawal/transfer of crypto funds via their VASP. To complete the transaction, the Client provides the Beneficiary blockchain address, the transaction amount, and Beneficiary ID Data.

2 Pre-verification of addresses: The VASP Originator checks the registered Beneficiary blockchain address with a blockchain analytics platform such as Coinfirm’s to see the risk associated with the address. High-risk addresses trigger a flag or block on the transaction and escalation to the VASP’s compliance department.

3 Propagation and verification of addresses to the VASP network: Once the address is risk checked, it should be propagated to the P2P network of VASPs. The network replies with information if the address belongs to any of them or not. Verification information should be consistent with the AML risk report and reviewed for any conflicting information about the ownership of the address.

4 Transfer of Travel Rule data: The withdrawal/transfer form pulls VASP and Client ID data from the VASP (Originator) database. The form also must inform the Client about the set of data that is transferred to the Beneficiary. In submitting the withdrawal/transfer request, the form serializes and pushes the data to the VASP (Originator).

5 Processing Transactions: The VASP (Originator) creates the blockchain transaction and pushes the Transaction Hash to the deployed FATF Software Kit. This creates and encrypts the Data Container and Data Container Signature with the PSK, thus creating an Encrypted Data Container with a heading equal to the Transaction Hash. It then pushes it to Coinfirm's TRAVEL Rule Solution API, thereby registering the Data Container timestamp, owner, and contents fingerprint on the public or private blockchain with additional information that prevents reversal of the hashing.



After validating the Beneficiary address and ownership, the encrypted Data Container is transferred via the FATF P2P Network exclusively to the node which has properly signed Beneficiary Address, successfully settling the transaction.

Any party (e.g., another VASP or regulatory authority) may use the Travel Rule Solution API to verify the Data Container to determine whether a given transaction meets FATF requirements.

Throughout this process, it is vital for VASPs and other obliged entities that engage in VA transfers to submit the required information securely to protect the customer information associated with the VA transfers. The solution proposed by Coinfirm in the report accomplishes that goal alongside the necessary transparency and risk assessment.

Conclusion

The issues surrounding the application of the Travel Rule to VASP-related transactions are complex. Some authorities have moved quickly to adapt existing legislation while others have taken a wait and see approach to monitor the development of solutions. The FATF continues to be engaged in discussions, but solutions have yet to be implemented, legislated for, and put in practical operation.

Given that such discussions will likely take some time, some people view the immediate adoption of standards and legislation in certain jurisdictions as an operational disadvantage compared to unregulated jurisdictions with lower transactional overhead. Coinfirm, however, advocates for a more pragmatic view. Adoption and implementation are a question of time. Many institutions, banks, service providers, working initiatives, and conglomerates have come together to try to begin to offer services and solutions; for both VASPs and local jurisdictions, a wait-and-see approach is no longer justified.

Appendix A: General Compliance Requirements

Policies and Procedures	KYC	Monitoring	Training	Responsibilities
Internal Procedure	Identification	Source of Wealth	Onboarding training	MLRO
Risk Assessment	Verification	Source of Funds	Annual training	Senior Management
Risk Based Approach	Sanctions	Ongoing Transactions Monitoring		Every Employee
	PEPs	Ongoing Profile Monitoring		Reporting
	Source of Funds / Source of Coins			SARs / STRs
Licencing	Negative News			Management Reports
	Enhanced Due Diligence			Record keeping

Appendix B - Acknowledgements

Complying with FATF Recommendations for Virtual Assets — Travel Rule was developed with a widely representative global working group of legal, regulatory, compliance, and technical experts spanning companies, industry groups, and government bodies.

- **Ruth Wandhöfer,** Independent Non-Executive Director LSE Group, Permanent TSB and Pendo Systems Inc; Partner Gauss Ventures; Senior Adviser KPMG
- **Dean Armstrong,** QC
- **James Brennan,** Duff & Phelps
- **Pawel Kuskowski,** Coinfirm
- **Diego Gutierrez,** IOV Labs/RSK
- **Yanmei Bi (Michelle),** Huobi
- **Martin Kopacz,** Xapo
- **Joey Garcia,** ISOLAS
- **Harry Saito,** Tokyo International Consulting K.K.

Coinfirm Ltd.

Lansdowne House (5th Floor), 57 Berkeley Square, London, W1J 6ER, United Kingdom
contact@coinfirm.com

For further information,

please contact:
report@coinfirm.com

Coinfirm is a global leader in compliance, regulatory and supervisory technology (RegTech and SupTech), creating a foundation for the safe and mass use of blockchain and cryptocurrencies. By providing solutions that fight fraud and allow regulated institutions to meet compliance requirements when interacting with virtual assets, we bridge the gap between the crypto and fiat currency worlds, enabling new monetary technologies to reach their full potential and contributing to the creation of a seamless, democratic and transparent financial system. The Coinfirm AML Platform sets the global standard for AML risk management and transaction analytics on blockchain with coverage of over 1300 public and private blockchains, cryptocurrencies, stablecoins and tokens (90%+ of the global market). The Platform also offers a solution for the FATF Travel Rule through a blockchain based utility allowing to securely store and transfer the identification data related to blockchain transactions.

Visit **www.coinfirm.com** to know more about our products and services.