Acuris Risk Intelligence

ospree

White Paper:

The Travel Rule: History and Requirement

Getting Ready for the Travel Rule with Ospree and Acuris

Crypto Catches the Eye of Regulators

During the past decade virtual currencies have become a well-known payment method and have become increasingly recognised around the globe for their flexibility, low costs and speed of transfer. The anonymity associated with them has alarmed regulators who have determined that blockchain technology creates conditions for wrong-doers to fund malicious activities or commit crimes, including money laundering and terrorist financing. The approach towards these cryptocurrencies is not universal – some countries have sought to encourage the virtual asset industry, albeit with the proper regulations, while others have adopted measures to restrict the use oreven ban cryptocurrency completely.

From a very early stage the Financial Action Task Force (FATF) identified the need to conduct detailed research intothese decentralised, mathematically based currencies (particularly Bitcoin) and assess the money laundering and terrorist financing risks associated with them. Even though FATF's recommendations are not legally binding, they are considered the gold standard for the AML/CFT efforts and best practices and are based on the national experience of the governments that form FATF's membership body. As early as June 2014, the international watchdog published a report, entitled Virtual Currencies – Key Definitions and Potential AML/CFT Risks. This industry-oriented report provided the common vocabulary and definitions associated with cryptocurrencies, how they can be classified, and who participates in such decisions.

How Cryptocurrency is Abused:

During the past decade, law enforcement authorities have documented many cases where criminals have taken advantage of cryptocurrencies' anonymous characteristics and have exploited them for illicit purposes. One example is the 2017 Wannacry ransom campaign in which hackers hijacked the computers of thousands of users and demanded that the victims pay ransom in Bitcoin in order to gain back access to their systems. More recently the attack on the American Colonial Pipeline ransomware attack exposed a fundamental misconception about Bitcoin, it is not so difficult to trace. However, an increase in the use of privacy wallets is being closely examined as they make transactions close to impossible to track, especially if performed in series. In March this year, a court casewas initiated against a Canadian-based company selling encryption devices that helped its clients transfer illegally obtained funds through cryptocurrencies.

Virtual assets have also attracted the attention of terrorist organisations as well. According to a 2019 report on the terrorist use of cryptocurrencies, prepared by RAND Corporation, the challenge involves not only Bitcoin but other currencies that have emerged after it and are

---

[1] "Virtual currencies – Key Definitions and Potential AML/CFT ... - FATF." https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Accessed 5 May. 2021.

[2] https://www.courtlistener.com/docket/59731822/1/united-states-v-eap/

challenge involves not only Bitcoin but other currencies that have emerged after it and are more private and secure, such as Omni Layer (MasterCoin), BlackCoin, Monero and Zcash. In August 2020, the U.S. Department of Justice announced that a terrorist financing network, relying on more than 300 cryptocurrency accounts to raise funds was dismantled in what was described as "the government's largest-ever seizure of cryptocurrency in the terrorism context".

Inception of the Travel Rule:

The first iteration of what we now call the travel rule was introduced in the US as the "Bank Secrecy Act" in the 1970, outlining a bank's data collection obligations to comply with government investigations into money laundering. Out of this act, SWIFT was born. In the decades that followed SWIFT became the international standard for data collection and sharing for institutional financial transactions worldwide.

As banking moved into the digital age, the Travel Rule has been refined and updated to remain useful and relevant to regulators and law enforcement in identifying financial crime.
Most notably, in October 2018 FATF amended its recommendations to apply to financial activities involving virtual assets. The international organisation also added two definitions – virtual asset (VA) and virtual assets service provider (VASP).

The new Recommendation 15 (New technologies) requires that VASPs fall within the scope of AML/CTF regulations and are "licenced or registered, and subject to effective systems for monitoring or supervision". Then in June 2019, the FATF adopted an 'Interpretative Note' to Recommendation 15 to provide further clarification on the risk-based approach that should be applied to VAs and VASPs, and to other compliance-related matters such as customer due diligence, recordkeeping, sanctions, and suspicious transaction reporting.

In the same month, a detailed guidance on the risk-based approach that should be applied to VAs and VASPs was released in order to help both state authorities and private sector companies offering virtual assets understand their obligations. The aim is to identify and prevent terrorists and other offenders from accessing electronically facilitated fund / wire transfers and using them to move and disguise illicitly obtained proceeds domestically and across borders.

The new and relevant addition to the 2019 guidance is the clarification that the FATF travel rule requirements extend out from the traditional financial sector and also apply to "VASPs that provide services or engage in activities, such as virtual asset transfers, that are functionally analogous to wire transfers".

Recommendation 16 should be applied regardless of whether the wire transfer is conducted in a fiat currency or a virtual asset. A de minimis threshold of USD/EUR threshold may be applied depending on the risks associated with virtual assets. In essence, the travel rule as we know it, and as it applies to cryptocurrency, is an update of the existing FATF Recommendation 16 which focuses on wire transfers.

According to Paragraph 7(b) of Recommendation 15, VASPs and other entities that conduct virtual assets transactions have to obtain, hold and transmit required originator and beneficiary information in order to perform their compliance-related obligations, such as identifying and reporting suspicious transactions, monitoring the availability of information, taking freezing actions, and prohibiting transactions with designated subjects.

---

[3] https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf
[4] https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns
[5] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
[6] http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

Additionally, FinCEN, the U.S. regulator competent on AML/CTF matters, amended its policy towards cryptocurrencies in May 2019 and defined VASPs as "money service businesses" which means that they have to comply with the Funds Travel Rule of the U.S. Bank Secrecy Act.

The required information includes name, account number; physical address or national identity number, customer identification number or other unique identity number, date of birth or place of birth; beneficiary's name and account number or virtual wallet number (where this is necessary to process the transaction).[1]

FATF[2]	**FinCEN**[3]
Requirements: Minimum Threshold USD/EUR 1000 Originator - Name - Account number - Physical address, or national identity number, or customer identification number that uniquely identifies the originator to the ordering institution, or date and place of birth. Beneficiary - Name - Account number	Requirements: Minimum Threshold USD 3000 Transmitter - Name - Account number - Physical address - Identity of the financial institution - Amount - Execution date Recipient - Name - Physical address - Account number - Any other specific identifier of the recipient

The progress of the new travel rule recommendations were monitored and in June 2020, a twelve-month review of FATF standards took place at the annual summer meeting, and in March 2021 FATF published their most recent draft of the Guidance for a risk-based approach to virtual assets and VASPs.

Among other matters, this updated draft Guidance was discussed at the FATF plenary meeting in June 2021 where it was reported that 52 out of 128 reporting jurisdictions are actively regulating VASP's for travel rule implementation4 FATF emphasised that all jurisdictions should implement the updated Travel Rule recommendations as soon as possible to avoid arbitrage.

---

[7] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[8] RBA for Virtual Assets & Virtual Asset Service Providers https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

[9] https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf

[10] "Outcomes FATF Plenary, 20-25 June 2021." https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2021.html. Accessed 17 Aug. 2021.

Response & Reception from Virtual Asset Service Providers

In practice, the Travel Rule is not without burden and restrictions on the entities that are obliged to comply with AML/CTF rules. Some cryptocurrency industry players have spoken up regarding three main concerns about its negative implications:

1. Philosophical objections:

The crypto Industry has been based on principles of decentralization and permissionless transfers of funds and tokens. This is one of the primary reasons many people started working in the field. The Travel Rule will require VASPs to become gatekeepers of whom their customers can transfer funds to. For many, this stands in opposition to the original philosophy of the industry.

2. Loss of business:

Explained by the "Sunrise Effect", some jurisdictions have relaxed or absent regulatory requirements pertaining to VASPS. Providers in more regulated countries will face additional complexities when dealing with their under-regulated counterparts; required KYC data may not be available and could therefore prevent the transaction from going through. This could cause a fraction in the virtual assets eco-system where only businesses operating in similarly regulated jurisdictions interact exclusively with one another.

3. Additional compliance costs

In most cases, implementing the travel rule adds friction and engineering costs to VASPs businesses. One of the biggest challenges is to collect all the data essential to comply with the travel rule; and then to aggregate that information from separate data silos. Companies who are not proactively taking these measures will incur significant costs and resources not only to access, process, and store the relevant information; but also, to obtain these details in a way that does not violate local privacy laws or disrupt their operation.

How Ospree & Acuris are working to solve the problem:

Ospree and Acuris Risk Intelligence have partnered and built an API integration in order to bring together the necessary KYC + KYT data to comply with the Travel Rule. Once a client is onboarded using Acuris to complete the KYC screening, they will show up in the Ospree dashboard where their wallets and transactions can be connected to their identity data. By connecting the identity of the user and their transaction you now have all the required data points securely assembled, and ready to be Travel Rule compliant.

This white paper was co-authored by Anne Winston, Ospree and Ralitsa Trifonova, Acuris Risk Intelligence.

---

[11]The Travel Rule for Crypto Businesses Report: https://f.hubspotusercontent00.net/hubfs/7222759/Travel%20Rule%20for%20Crypto%20Businesses%20Report%20June-22-2020.pdf?__hstc=152266662.59569cca29a4361b9f6042ccafc9f45b.1622614547524.1622614547524.1622616626314.2&__hssc=152266662.3.1622616626314&__hsfp=289446713