

**From:** [John Jefferies](mailto:John.Jefferies@federalreserve.gov)  
**To:** [regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov)  
**Subject:** Docket No. R-1726; RIN 7100-AF97  
**Date:** Friday, November 27, 2020 6:26:38 PM

---

NONCONFIDENTIAL // EXTERNAL

TRISA Feedback on Docket No. FINCEN-2020-0002 ; RIN 1506-AB41

November 27, 2020

US Federal Reserve and FinCEN Proposed Rule Change

Regarding: Docket No. FINCEN-2020-0002 ; RIN 1506-AB41

Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving CVCs

To: Board of Governors of the Federal Reserve System (“Board”); Financial Crimes Enforcement Network (“FinCEN”), Treasury.

Regarding: Joint notice of proposed rulemaking.

Summary of Proposed Recommendation:

Harmonize all Travel Rule regulations at \$1,000

Waive address requirement for virtual currency travel rule compliance

Allow twelve months for VASPs to comply

Background

The proposed rule change would reduce the information collection, retention, and transmission threshold from \$3,000 to \$250 for funds transfers and transmittals of funds that begin or end outside the United States. The Travel Rule Information Sharing Alliance (TRISA) is an organization of more than a hundred stakeholders including exchanges, Bitcoin ATMs, compliance experts, regulators, privacy coin advocates, and technologists. We applaud the rulemaking process to achieve clarity.

It had previously been unclear if the travel rule applied to CVCs in the US. Clarifying the meaning of “money” as used in these same rules to ensure that the rules apply to domestic and cross-border transactions involving convertible virtual currency (“CVC”), which is a medium of exchange (such as cryptocurrency) that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status, is laudable.

The proposed changes generate several issues to which TRISA collectively proposes recommendations.

Issues:

Issue 1: Inconsistencies with FATF guidance for global de minimis Travel Rule threshold

Inconsistencies between the FinCEN proposal and FATF recommended thresholds for application of the Travel Rule will unduly complicate an already difficult compliance challenge by requiring conditional processing and cause increased exception handling. Complying with the FinCEN \$3000 threshold for domestic CVC transfers, which is inconsistent with FATF’s \$1000 threshold for all transactions is already confusing. Adopting a \$250 threshold for international transactions will have the perverse impact of driving bad actors towards unregulated, nonreporting unhosted wallets. The \$250 threshold impedes financial inclusion by creating hurdles for personal remittances.

Recommendation 1: Harmonize all Travel Rule regulations at \$1,000 for all CVC transfers between VASPs.

Issue 2: Difficulty of determining if an address is cross border based on the location of VASP

It is for this reason that the FATF decided in its virtual asset guidance that “countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations.”

Recommendation 2: Treat all virtual asset transfers as cross border.

### Issue 3: Sending address and tax information on US persons to untrusted VASPs

The proposed threshold reduction from \$3,000 to \$250 for funds transfers and transmittals of funds that begin or end outside the United States will result in the sharing of sensitive US PII with unknown or untrusted VASPs, creating numerous privacy issues for virtual asset users. As evidenced by dozens of successful exchange hacks, few VASPs are well prepared to defend against a dedicated adversary and have poor security around crypto assets, let alone stored PII.

Many smaller VASPs have minimal security expertise and have previously not considered themselves to be financial institutions. Risks to individual privacy, and to individuals, in the context of the Travel Rule include exposing sensitive PII to VASPs pursuant to the instructions of the Travel Rule where the receiving VASP is vulnerable to :

- Hacks and PII data leaks
- Fake VASPs masquerading as legitimate VASPs to collect PII
- Harvesting, data mining, and selling user PII data
- Monitoring by oppressive regimes, leaks, hacks, data mining, poor security, and data brokering
- DDOS and market manipulation

Recommendation 3: Eliminate the requirement to send address information and SSN/EIN for CVC travel rules.

### Issue 4: Time to comply

Very few VASPs in the United States have implemented a travel rule technical solutions in production environments. The state of travel rule compliance solution implementation globally would best be described as very early stage with a few Minimal Viable Products at the beta test phase. Adequate time needs to be allotted to avoid negative privacy implications when transacting with VASPs with less rigorous operational security and potentially vulnerabilities.

Recommendation 4: Continued regulatory forbearance. Provide a twelve-month safe harbor window for VASPs that are able to demonstrate progress in implementing and actively integrating MVP/POCs. We further recommend a record-keeping period in the interim when data is collected and retained but not transmitted.

### Issue 5: Cost of compliance significantly underestimated

In the first three years, exception handling and implementation will cost considerably more than estimated. Information technology implementation costs solely resulting from the need to comply with this proposed ruleSoftware and operational costs for a large to medium-sized MSB will be over could easily cost between \$500,000 and \$100,000 for commercially supported software and required security infrastructure.

VASPs outside of the US will also bear additional costs of compliance if they transact with US persons and may choose not to so, thereby denying US persons with access to exciting new technology and costs savings.

Recommendation 5: Support the global standard of \$1000 to reduce conditional processing and costly manual exception handling.

Thank you for the consideration,  
TRISA Board of Directors

### Appendix 1

Decreasing the threshold to collect, retain, and transmit information on the transmittals of funds that “begin or end outside the United States” would increase the number of transactions that trigger Travel Rule thresholds every year by a factor of at least 2.5, according to CipherTrace analysis.

### Minimum Monthly Travel Rule Transactions

According to CipherTrace data, to comply with the current US Travel Rule threshold of \$3,000, US VASPs would have had to have sent over 34,000 messages during the month of October. Over 27,000 of these messages—around 78%—would have been cross-border in nature, meaning the sending or receiving VASP was domiciled outside of the United States. This would translate to over 417,000 messages a year at the current threshold.

Lowering the threshold to \$250 would push the number of required travel rule messages to be shared and stored per year to over one million. At this lower threshold, cross-border transactions make up 83% of all travel rule triggers for US VASPs.

US VASP Travel Rule Triggers	Current 3k	Proposed Change
US Domestic only	7500	7500
Cross US Border	27300	79000
Monthly Travel Rule Triggers	34800	866500

If the US were only to lower its threshold to FATF’s de minimis standard of \$1,000, then the number of transactions that would trigger compliance would only increase by a factor of 1.7 every year.

Intermediary banks or financial institutions are also required to transmit this information to other banks or nonbank financial institutions in the payment chain. The proposed rule change acknowledges that cryptocurrency can be transferred without third-party bank involvement but states that, in reality, many users rely on hosted wallets and exchanges to transact.

#### Difficulty in determining “cross-border payments” in the virtual asset world

FinCEN’s proposed rule change is based on transactions that “begin or end outside the United States.” These transactions are defined by whether a financial institution “knows or has reason to know that the transmitter, transmitter’s financial institution, recipient, or recipient’s financial institution is located in, is ordinarily resident in, or is organized under the laws of a jurisdiction other than the United States or a jurisdiction within the United States.”

Due to the cross-border nature and global reach of virtual assets and VASPs, compliance with this definition would be difficult to enforce, especially given many VASPs are often registered in multiple jurisdictions around the world. A financial institution would only have “reason to know” that a transaction begins or ends outside the United States to the extent that such information was shared when receiving the transmittal order or collected from the transmitter —assuming he or she even knows the true extent of the cross-border nature of their transaction.

It is for this reason that the FATF decided in its virtual asset guidance that “countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations.”

#### Appendix 2

Travel Rule Information Sharing Alliance Introduces Critical Infrastructure to Address Interoperability Issues Presented by the FATF’s Travel Rule Requirements

TRISA VASP Directory and TRISA Certificate Authority to overcome the sunrise problem by bootstrapping trusted communication with Mutual VASP Authentication.

MENLO PARK, Calif., Aug. 20, 2020 — Travel Rule Information Sharing Alliance (TRISA.io) releases V8 of its whitepaper introducing the global TRISA VASP Directory and the TRISA Certificate Authority to enable Virtual Asset Service Providers (VASPs) to bootstrap trusted information sharing and comply with pending Travel Rule laws. The critical infrastructure presented by TRISA helps VASPs overcome the sunrise problem, empowering counterparties to establish trusted communication across jurisdictions that enforce Travel Rule regimes on different timelines.

TRISA also formalized governance, announcing the board of directors who have agreed to form a nonprofit. TRISA board members include John Jefferies as Chairman, CEO of CipherTrace Dave Jevans, Senior Software Research Engineer at Ripple Aanchal Malhotra, Chief Compliance Officer at Paxful Lana Schwartzman, Thomas Hardjono of MIT Connection Science & Engineering, and Chair of Blockchain and Digital Assets Practice at Bradley Carol van Cleef who is also founder and CEO of Luminous Group, a blockchain and cryptocurrency consulting firm.

John Jefferies, Chairman of TRISA, said, “In light of the recent OCC ruling allowing US banks to provide custody services for cryptocurrency assets, those that hold cryptocurrency will need to abide by the Travel Rule. Banks currently lack the infrastructure to comply with the Travel Rule when it comes to cryptocurrency transfers and must learn to share Travel Rule information with exchanges, funds, and non-custodial wallets.”

Lana Schwartzman, Chief Compliance Officer at Paxful, shared, “I’m thrilled and honored to join this board. TRISA has been on the forefront of Travel Rule implementation since version 1 of the white paper. They were able to show forward progress to FATF for VASPs seeking to comply with the Travel Rule globally by focusing not only on security, but interoperability as well which is essential to the success of the rule.”

Thomas Hardjono of MIT Connection Science & Engineering expressed, “The TRISA information sharing alliance provides the foundation for the nascent VASP and virtual assets industry to develop the next-generation trust infrastructure for future global finance, providing not only information assurance and reliability, but also compliance to the global AML/FT regulations.”

Among outcomes from June’s Financial Action Task Force (FATF) Plenary meeting was the need for a global solution that allows VASPs to meet the FATF’s Travel Rule guidelines across regulatory jurisdictions. The Travel Rule requires VASPs to share certain sender and receiver information for cryptocurrency transactions such as names and account numbers of both parties and either the originator’s physical address, national id number, customer id number, or date and place of birth.

TRISA has implemented InterVASP Message Standard 101 (IVMS) to standardize Travel Rule message data fields. Several Travel Rule approaches have emerged, and many have converged on IMVS as a foundational layer, but limited scope and non-standard messages hinder globally-compatible information sharing. Version 8 of the TRISA whitepaper describes how interoperability among different protocols, message flows, and data types will be enabled with a Translation Interface. This interpreter function is critical to automating and scaling cross-border solutions for VASPs seeking to comply with global Travel Rule standards.

TRISA’s solution features the TRISA VASP Directory, which includes location data and contact information on 800 VASPs. The directory will assist VASPs in determining if meeting a given request to share sensitive information, per Travel Rule requirements, is safe and compliant. The expanded directory will include answers compiled from the TRISA Questionnaire developed in collaboration with Global Digital Finance and the Digital Chamber of Commerce. The purpose of this questionnaire is to provide a common set of questions VASPs can ask other VASPs with whom they are planning to begin exchanging Travel Rule information.

“CipherTrace donated the initial directory data set to help TRISA Alliance members make informed compliance decisions before sending or receiving large sums of virtual assets,” explained Dave Jevans, Co-Chairman of TRISA and CEO of CipherTrace. “The directory will be augmented with entity details, regulator and licensing information, Travel Rule vectors, and privacy information.”

The TRISA Certificate Authority will issue X.509 certificates to TRISA members, which will be used for mutual VASP authentication of TRISA members, ensuring confidential sharing of information between entities. The certificate authority will also issue Extended Validated (EV) KYC certificates after verifying business details. The root certificate from the TRISA Certificate Authority is embedded in the TRISA source code and will ensure that only instances with valid certificates can interact with other valid instances.

#### About TRISA

Travel Rule Information Sharing Alliance (TRISA) is an open-source framework to support VASPs in sharing sender and receiver information to comply with Travel Rule requirements without compromising privacy. By applying a proven Certificate Authority (CA) model, TRISA reliably identifies and verifies VASPs to enable interoperability and ensure Personally Identifiable Information (PII) stays private and not sent to the wrong entity. The peer-to-peer design eliminates a single point of failure and provides resilience against attacks and scales to accommodate extreme volumes. VASPs and financial institutions can immediately begin using TRISA to comply with the Financial Action Task Force (FATF) and Bank Secrecy Act (BSA) requirements as well as Travel Rule guidelines.