

**From:** [John Jefferies](mailto:John.Jefferies@federalreserve.gov)  
**To:** [regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov)  
**Subject:** Re: Docket No. FINCEN-2020-0002 RIN 1506-AB41 - CipherTrace Feedback - Docket No. R-1726; RIN 7100-AF97  
**Date:** Friday, November 27, 2020 11:51:50 PM  
**Attachments:** [image001.png](#)

---

NONCONFIDENTIAL // EXTERNAL

Docket No. R-1726; RIN 7100-AF97

---

**From:** John Jefferies <jj@ciphertrace.com>  
**Date:** Friday, November 27, 2020 at 3:47 PM  
**To:** "regs.comments@federalreserve.gov" <regs.comments@federalreserve.gov>  
**Subject:** Docket No. FINCEN-2020-0002 RIN 1506-AB41 - CipherTrace Feedback

November 27, 2020

Via Email to: [regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov)

Policy Division  
Financial Crimes Enforcement Network  
US Department of the Treasury  
P.O. Box 39  
Vienna, VA 22183

**Re: FinCEN Docket Number FINCEN–2020– 0002; RIN number 1506–AB41**

CipherTrace welcomes the opportunity to comment on the Financial Crimes Enforcement Network (“FinCEN”)’s proposed rule change regarding the “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 Convertible Virtual Currencies and Digital Assets With Legal Tender Status.”

Leading cryptocurrency intelligence company CipherTrace protects financial institutions from crypto laundering risk and is helping to grow the crypto economy by making virtual assets trusted by governments and safe for mass adoption. We deliver the world’s most comprehensive cryptocurrency intelligence to detect money laundering, perform financial investigations, monitor risky payments and enable regulatory supervision. Our founders are dedicated to protecting consumer privacy, while defending against illicit finance. Deep expertise in cybersecurity, eCrime, payments, banking, encryption, and virtual currencies form the foundation for CipherTrace’s commercial offerings

We look forward on our continued collaborating with FinCEN in this and future endeavors.

### ***Proposed Reduction of Recordkeeping and “Travel Rule” Threshold***

The proposed rule change intends to lower the existing dollar threshold in 31 CFR 1020.410(a) and 31 CFR 1010.410(e) and (f) to collect, retain, and transmit information on funds transfers and transmittals of funds in amounts of \$3,000 or more to \$250 for funds transfers and transmittals of funds that begin or end outside the United States.

According to the published document (2020-23756), the data used to derive this new, lower threshold was based on SAR filings related to fentanyl trafficking or potential terrorist financing-related transmittals of funds. According to the data, 57% of terrorism financing related transmittals were at or below \$300, with 99% being cross-border in nature. Additionally, over 82% of fentanyl trafficking

SARs involved cross-border transmittals, with 52% being at or below \$300.

There is inherent bias to this data set used to calculate the \$250 threshold. As transactions at those low amounts are below thresholds for required SAR filing, institutions generally only file on transactions this low (i.e. \$250) when they are confident of criminal activity and have actionable intelligence on the crime. This means that the percentage of actionable SARs at \$250-\$300 is significantly larger than the data lake of SARs that are filed at or above this threshold. This means under transaction SARs are much better quality than over threshold SARs that are mostly filed by FIs or NBFIs as a "just in case" CYA move.

While CipherTrace recognizes that lowering the threshold to capture smaller-value cross-border funds transfers and transmittals of funds may initially appear valuable for law enforcement and national security authorities, we believe that, as it pertains to the cryptocurrency sphere, the combination of an immutable blockchain and proper suspicious activity reporting programs are adequate enough to mitigate FinCEN's concerns.

In 2019, MSBs filed 852,925 SARs and FIs filed 1,116,400 SARs. Those data lakes are large, and the utilization of the information is not always effective.

### ***The Difficulties VASPs Face in Identifying Cross-Border Transactions in Crypto***

Unlike traditional financial institutions, the virtual currency industry faces unique challenges regarding FinCEN's funds transfer rule—most notably, the challenge in identifying a) when a counterparty is another virtual asset service provider and b) identifying where that virtual asset service provider is domiciled.

Identifying when a counterparty is another financial institution isn't as simple in the crypto sector as it is in the formal financial sector. With cryptocurrencies, it is not only banks and other financial institutions initiating and receiving transfers. Application of the funds travel rule means VASPs face the distinct dilemma of needing to identify and verify whether or not a beneficiary cryptocurrency address belongs to another VASP. To make matters more complicated, VASPs are constantly adding new deposit addresses and, unlike routing numbers or SWIFT codes, there is no clear connections between these new addresses and their respective VASP without the use of blockchain analytics.

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.

Determining the actual domicile of a centralized VASP further complicates the determination of "cross-border" transfers. Unlike traditional institutions, one VASP may support many countries and regions without the need to create distinct "branches" per jurisdiction. Likewise, some VASPs purposely chose to domicile in regions where AML regulations are more lax, despite most of their customer base residing outside of their official domiciled jurisdiction. The global make-up of the customer bases of these VASPs disrupt the purpose behind identifying cross-border transfers in the first place. Unlike centralized VASPs, decentralized VASPs—or decentralized exchanges—often times won't even have a central body, which allows them to be truly global.

Because of this cross-border nature of VA activities and VASP operations, the FATF determined in their *Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* 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.” CipherTrace recommends that FinCEN treat all cryptocurrency transfers as cross-border. Adoption of this standard would help US-based VASPs more easily comply with their new and existing obligations under the BSA.

***Technology and Startup Costs: A 92% Threshold Reduction Results in 150% Increased Burden on VASPs***

The proposed reduction for Travel Rule compliance is a significant shift that would lower the threshold for record keeping and “Travel Rule” message transmittals by nearly 92%. CipherTrace has calculated that this change would increase the number of transactions that trigger Travel Rule compliance every year by a factor of at least 2.5.

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.

Region	Monthly US Transactions			Number of "Travel Rule" Messages Required by US VASPs		Transactions at FATF Threshold (\$1,000)	
	txs over \$250	txs over \$1,000	txs over \$3,000	Current	Proposed Change	US	Other
US Domestic	15,921	11,016	7,510	7,510	7,510	11,016	
US Cross-Border	79,011	46,780	27,295	27,295	79,011	46,780	
International (Non-US)	392,952	260,439	178,664				260,439
Global	487,884	318,235	213,469				
<b>Monthly Travel Rule Messages</b>				<b>34,805</b>	<b>86,521</b>	57,796	260,439
<b>Annual Travel Rule Messages</b>				<b>417,660</b>	<b>1,038,252</b>	693,552	3,125,268

Source: CipherTrace Cryptocurrency Intelligence

The proposed change would increase the volume of required Travel Rule messages by 150% (2.5x). As a result, US VASPs will likely incur significant additional expenses, such as an increased compliance personnel, increased technical resource costs, and the loss of revenue due to the slowing down of the transactional process. Cryptocurrency users often need and require quick transactions in order to take advantage of market conditions. Slowing those transactions down would greatly impact the crypto economy.

These are only a few examples of the potential impact of the proposed rule change. The 30-day comment window provided is insufficient time for Virtual Asset Service Providers to fully calculate the impacts the lowered threshold. These changes come as many in the industry are still developing their “Travel Rule” compliance strategies, which already requires the use of new technologies and processes to collect and send the required information.

### ***Safe Harbor for Travel Rule Compliance***

The uneven adoption of cryptocurrency “Travel Rule” provisions outside of the United States creates a potentially dangerous circumstance for US VASP customers whose data is transmitted to non-FATF-compliant jurisdictions.

CipherTrace suggests that FinCEN provide US VASPs with a “Safe Harbor” exemption for transmitting “Travel Rule” data until an operational system is in place. Similar “Safe Harbor” exemptions have been implemented by FinCEN before; most notably in 1998, shortly after first implementing the “Travel Rule.” We believe FinCEN should extend the same administrative flexibility to VASPs that it extended to financial institutions in 1998, as leaders in the cryptocurrency sector continue to develop the appropriate means of compliance.

There has been much progress in the past year as global leaders in the cryptocurrency sector continue to work together to develop appropriate solutions for “Travel Rule” compliance following FATF’s “Travel Rule” announcement last June.

### ***Final Thoughts—Adopting a FATF Level Threshold***

CipherTrace believes adopting a \$1,000 threshold for cross-border transfers would be consistent both with FATF requirements and with FinCEN’s own proposed rules for domestic transactions. Law enforcement interests in tracking information associated with lower-dollar transactions that cross borders can be achieved using suspicious activity report (SARs) and other existing reporting obligations, without creating undue burdens on VASPs and their customers. Harmonizing all Travel Rule regulations at \$1,000 and treating all crypto asset transfers as cross-border would help US-based VASPs more easily comply with their new and existing obligations under the BSA.