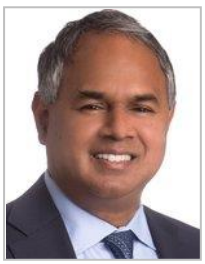
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FinCEN 'Travel Rule' Update Sets Challenges For Crypto Cos.

By **Katherine Kirkpatrick, Jeffrey Telep, Shaswat Das and Jacob Gerber**
October 11, 2019, 5:28 PM EDT

Katherine Kirkpatrick

Jeffrey Telep



Shaswat Das

Jacob Gerber

The regulation known as the "travel rule," first issued by the Financial Crimes Enforcement Network in 1995 with fiat currency in mind (and amended in 2013 to include electronic funds transfers), requires banks and nonbank financial institutions to transmit information on funds transfers and transmittals of funds to other banks or nonbank financial institutions.

Guidance in May and June from the Financial Action Task Force and FinCEN expanded the application of the travel rule to a new area, virtual currencies, and the industry has just now begun to formulate compliance solutions to these new and potentially problematic regulatory obligations.

Some companies in the sector are looking to blockchain technology for a travel rule compliance solution. In September, CipherTrace Inc. proposed a parallel network operating alongside Bitcoin and other virtual currency protocols.

At least in theory, it should be possible to build a secure network among money service businesses to transmit the information required by the travel rule — customer identification and transaction details. If one platform for compliance attains a critical mass, pressure on other crypto asset business to participate could create momentum and lead to broader market adoption.

However, even recent solutions do not provide a foolproof plan going forward. Any errors in implementing a parallel network would create serious user-data privacy concerns in an industry where confidentiality is valued at a premium.

Further, if such a compliance network went offline — whether from malicious attack or system error — all money service business virtual currency transfers over a nominal threshold would have to cease or risk noncompliance.

Regulators have said the expansion of the travel rule is meant to level the playing field between different financial platforms. In reality, the inherent difference between conventional platforms and cryptocurrency platforms, especially in light of the pseudonymous nature of wallet addresses, makes compliance with the travel rule exceptionally challenging for virtual currency businesses.

At the moment, while a number of third-party service providers are developing potential solutions to comply with this change, it remains to be seen what compliance mechanisms, tools or protocols will emerge to be the most effective in the near term.

New Application of The Travel Rule — Virtual Currencies

In the first half of 2019, both FATF and FinCEN announced regulatory guidance to apply the travel rule to virtual currency businesses.

FATF Guidance on the Travel Rule

In February, FATF[1] solicited public comments on a proposal to apply its version of the travel rule to virtual currency businesses, which are referred to as "virtual asset service providers," or VASPs, by FATF.[2] Interest groups and businesses responded with concerns and specific practical obstacles about applying the travel rule outside of traditional banking,[3] but nevertheless, in June, FATF adopted its original proposal.[4]

As defined by FATF, VASPs include any person or entity that provides any of the following services to others as a business:

1. Fiat and virtual asset exchange;

2. Exchange between virtual assets;

3. Transfer of virtual assets;

4. Safekeeping of virtual assets; or

5. Activities related to issuing or underwriting virtual assets.[5]

FATF's rule covers transfers undertaken on behalf of a customer either between two VASPs, or between a VASP and a financial institution otherwise covered under the rule. The travel rule still applies to transactions between a VASP, such as a virtual currency exchange, and a traditional financial institution, such as a retail bank.

Just as an example, consider a virtual currency transfer from one VASP to another VASP, undertaken on behalf of a customer. If the transaction is for the equivalent of more than one thousand U.S. dollars or Euros, the originating VASP is required to obtain, hold and transfer to the beneficiary VASP the following information:

1. The originating customer's verified name;

2. The originating customer's verified account number;

3. The originating customer's verified physical address, national identity number, or date and place of birth;

4. The beneficiary customer's name; and

5. The beneficiary customer's account number.[6]

Although FATF guidance does not have the force of law, FATF member countries almost universally implement laws based closely upon its recommendations. In the U.S., FinCEN issued guidance in May applying the travel rule to virtual currency businesses.

FinCEN Application of the Travel Rule to Money Service Businesses and Convertible Virtual Currencies

In May 2019, FinCEN released long-awaited guidance on the application of existing anti-money laundering rules, including the travel rule, to virtual currency businesses.[7] According to the FinCEN guidance, money service businesses transmitting value equivalent of $3,000 or more must include the following information in a transmittal order:

1. The transmitter's name;

2. The transmitter's account number;

3. The transmitter's address;

4. The identity of the financial institution;

5. The amount transferred; and

6. The date of transfer.

In contrast to FATF's guidance, FinCEN clarified that the recipient's financial institution should retain the same information as the originator to the extent that the information has been provided by the originating money service business.

The differences between the FATF and FinCEN guidance are limited, aside from the transaction thresholds: $1,000 (FATF) and $3,000 (FinCEN).

Key Challenges for Virtual Currency Businesses to Comply With the Travel Rule

Virtual currency businesses face significant obstacles in complying with the travel rule. First, compliance requires the collection of information that is not essential to completing a virtual currency transaction. Further, as currently designed, virtual currency businesses attempting to comply with the rule do not always have all of the information necessary to determine which transactions are covered.

The information necessary to complete a Bitcoin[8] transaction, for example, includes the recipient's address and the amount of the transaction — and this information alone does not indicate whether the recipient is a VASP or money service business, which is essential for determining whether the travel rule applies.

Additionally, systems to support compliance run the risk of creating serious transactional bottlenecks. Finally, in the world of virtual currencies, the travel rule is susceptible to circumvention, as explained further below.

Mismatch of Transaction Requirements and Regulatory Requirements

When the travel rule was originally enacted for bank-to-bank transfers, the information required under the rule was substantially the same as the information already required to complete the transfer itself. Originally, the most significant feature of the travel rule was not the collection of any additional information, but rather the requirement to transfer that information to the recipient and the requirement to retain the information in case of subsequent government inquiries.

But applying the travel rule to cryptocurrency exchanges and other virtual currency businesses can be burdensome because it requires the collection and retention of information that is not required for the underlying transfer.

By design, virtual currency transactions require less information than a traditional bank-to-bank transaction. For a virtual currency transaction, all that is required is the originator's virtual currency address, the beneficiary's virtual currency address and the amount to transfer.

Applying the travel rule would burden virtual currency transactions between VASPs with the obligation to collect nonessential information like the recipient's name and address. With respect to bank-to-bank transfers, this would be tantamount to the original travel rule requiring banks to obtain, transmit and retain information on a transaction's purpose, even though this is not inherently necessary (though required by some banks) to complete the transaction.

Information Deficits for Sender and Recipient are Compliance Obstacle

Under the FATF and FinCEN rules, compliance is only required where funds are transferred on behalf of a client or customer. However, with respect to VASP-to-VASP transfers, VASPs often have no way to know when they are transferring virtual currency to another VASP or receiving virtual currency from another VASP.

Without this information, VASPs cannot distinguish which transactions fall under the travel rule and which ones do not.

Theoretically, the information required by the travel rule could be built into new fields within the Bitcoin protocol, but there are two practical obstacles.

First, VASPs and other covered financial businesses do not have the authority/ability to modify the Bitcoin protocol.

Second, the parties that do have the authority/ability to modify the Bitcoin protocol (programmers that propose changes, Bitcoin miners that decide whether to support and adopt those changes) value privacy, confidentiality, and coding efficiency. Thus, they would be unlikely to support changing the protocol to enable compliance with the travel rule, as the changes would undermine those values.

Use of a Parallel System Based on Centralized Authority for Travel Rule Compliance Could Threaten Data Security and Transactional Reliability

Blockchain forensics firm CipherTrace has very recently proposed a new system, independent of the Bitcoin protocol or any other virtual currency protocol, to enable travel rule compliance for VASPs.[9] But if not properly designed or executed, such a system could threaten user information privacy. A VASP

could send information required under the travel rule to the wrong party if the proposed system incorrectly identified the owner of the recipient account.

A parallel system could also threaten to leave VASPs, including major exchanges, unavailable during any downtime. For example, if this parallel system were targeted with a distributed denial-of-service attack[10] and became unavailable, VASPs may be prevented from executing any external transfer requests. VASPs would have no way to determine if a requested transaction fell under the travel rule or not until the system came back online. VASP transactions with external parties could be blocked for reasons extrinsic to any virtual currency protocol.

Virtual Currencies Make the Travel Rule Easy to Circumvent

Another concern is user compliance with the expanded rule, as individual users will be able to easily circumvent the travel rule as applied to VASPs. The rule only applies to transfers between VASPs (or other financial institutions) taken on behalf of a customer. To avoid these transfers, a customer could simply direct a transfer from a VASP to an individual account, and then direct a second transfer from that individual account to the second VASP. Alternatively, users could avoid the travel rule by avoiding VASPs altogether using peer-to-peer transactions.

Conclusion: Unintended Consequences and Unintended Benefits

Currently, it is unclear if the virtual currency sector will find a practical way to comply with the travel rule. Although no parties have proposed an elegant compliance solution, virtual currency businesses may work together to find a workable path forward. If businesses do find a way to comply, regulators may find both unintended consequences and unintended benefits.

Regulator and law enforcement oversight of the virtual currency sector could suffer if the travel rule leads users to avoid VASP-to-VASP transfers. Globally, government offices rely on financial institutions to provide visibility and insight into market changes and transaction flows. Policies, like the travel rule, may suppress financial innovation and ultimately limit government access to information from certain financial businesses.

However, if the virtual currency business community is able to devise a system for travel rule compliance, user circumvention may provide law enforcement with new investigative opportunities. If individuals trying to avoid detection by law enforcement change transaction patterns, and if the majority of users make no change in their transaction patterns to avoid the travel rule, investigators may be able to generate leads based on this distinction.

A similar dynamic arose in narcotics trafficking enforcement. Traffickers have gone to extreme lengths to avoid transactions requiring currency transaction reports. However, while they have been successful at avoiding CTRs, their tactics have left other patterns for investigators to find, such as a series of small deposits by a single person at a string of local banks in a short amount of time. With respect to the travel rule, the upshot is that individuals trying to circumvent the compliance requirements may expose themselves by leaving other distinct patterns for investigators to detect.

Ultimately, this may be a case where regulators and the virtual currency community can come together to find a practical middle ground. Even if the travel rule is unworkable in its current form, as noted above, there are ongoing efforts to leverage blockchain analytic tools to promote compliance with the rule. Virtual currency businesses can help prevent money laundering in other ways. Strong "know-your-

customer" policies and practices are essential to provide law enforcement and regulators information on suspicious transactions.

Faced with these new obligations, it is important for businesses to employ all practicable efforts to quell risks associated with virtual currencies. Industry participants should be cognizant of these new requirements and examine their own infrastructure. Companies would be well advised to obtain the advice of counsel with a broad experience in traditional AML compliance and in the burgeoning world of virtual currency compliance.

Katherine Kirkpatrick and Jeffrey Telep are partners, Shaswat K. Das is counsel and Jacob Gerber is an associate at King & Spalding LLP.

Matthew Wissa, an associate at the firm, contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] The Financial Action Task Force is an intergovernmental organization devoted to combating money laundering and terrorism financing. In recent years, FATF has proposed regulations on cryptocurrencies for its 37 member nations. See FATF, Who We Are (Sept. 25, 2019), https://www.fatf-gafi.org/about/.

[2] FATF, Public Statement: Mitigating Risks from Virtual Assets, Draft Interpretive Note to FATF Recommendation 15 (Feb. 22, 2019), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

[3] Global Digital Finance, Comment Letter to FATF Regarding Public Statement Dated Feb. 22, 2019 (April 7, 2019), https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf; Chainalysis, Comment Letter to FATF Regarding Interpretive Note to Recommendation 15 (April 8, 2019), https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis_Input_7b_Public_Statement.pdf.

[4] FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 21, 2019), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

[5] Id. at 57.

[6] Id. at 29. The beneficiary VASP must obtain and hold verified information about the beneficiary, but is not responsible for verifying information about the originator.

[7] FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[8] Bitcoin is a decentralized virtual currency based on distributed ledger technology. Bitcoin users can make transfers directly to other users without the assistance of a bank or any other financial institution.

The record of past transfers is maintained on a distributed ledger. The ledger is updated by consensus, not by a central authority.

[9] Cipher Trace, Travel Rule Information Sharing Architecture for Virtual Asset Service Providers (TRISA) (Aug. 22, 2019), https://ciphertrace.com/wp-content/uploads/2019/08/TRISA-Enabling-FATF-Travel-Rule-V4.pdf; see also Anna Baydakova, Chainalysis Hires FinCEN Vet to Tackle Crypto's New 'Travel Rule' Challenge, Coin Desk, (Jun 26, 2019), https://www.coindesk.com/chainalysis-hires-fincen-vet-tackle-crypto-travel-rule-challenge.

[10] A distributed denial-of-service attack is designed to overwhelm a targeted website, server, or internet platform with an exceptionally high volume of internet traffic, with the goal of making the target unavailable to normal users.