ComplyFirst

TRAVEL RULE COMPLIANCE

Summary

FinCEN issued guidance in May 2019 to remind those subject to the Bank Secrecy Act (BSA) how FinCEN regulations apply to Virtual Asset Service Providers (VASPs). This guidance is therefore likely applicable to certain cryptocurrency exchanges, among other parties, who are considered VASPs. This guidance reminds VASPs that among other things, certain activities they perform may be subject to the Funds Travel Rule. Non-regulated entities (typically the case for peer-to-peer transfers between two individuals) are not subject to these requirements.

FinCEN's May 9, 2019 Guidance

The guidance issued by FinCEN available here did not establish new regulatory expectations or requirements. Rather, existing guidance and regulations are consolidated and applied to VASPs dealing with convertible virtual currencies (CVC).

One of the points noted in the guidance is that to the extent that a money transmitter's transactions constitute a transmittal of funds according to the FinCEN regulations, the money transmitter must also comply with (among other things) the Funds Travel Rule.

What is the Funds Travel Rule?

The Funds Travel Rule requires VASPs who are sending and / or receiving funds to or from other financial institutions to capture, transmit, and store certain information associated with each transfer of funds above a certain threshold.

Referencing these documents by the SEC and FinCEN:

- Only transmittals of funds equal to or greater than $3,000 (or its foreign equivalent) are subject to the rule.
- A transmittor's financial institution must include and send the following in the transmittal order:
    - The name of the transmittor
    - The account number of the transmittor, if used
    - The address of the transmittor
    - The identity of the transmittor's financial institution
    - The amount of the transmittal order
    - The execution date of the transmittal order, and
    - The identity of the recipient's financial institution
- A receiving financial institution must receive and retain:
    - The name of the recipient
    - The address of the recipient
    - The account number of the recipient, and

- Any other specific identifier of the recipient

Regulated exchanges that are currently AML / KYC compliant should have most of the information required to transmit when appropriate since they retain certain customer identification documentation as part of their AML / KYC processes. Additionally, details of specific transactions are presently displayed on most major exchanges in the relevant "user account," "transaction history," "ledger," or other appropriate heading, meaning that most of the required data is probably already being captured. Transaction IDs are searchable in the public blockchain if available. Or, if the cryptocurrency under question is a privacy-preserving cryptocurrency there are other methods to obtain transaction information beyond what the exchange may have, which we detail in our compliance briefs.

Some jurisdictions may impose stricter requirements. Switzerland's FINMA, for example, requires that exchanges send and receive funds only from verified ("whitelisted") addresses (emphasis ours):

> "Institutions supervised by FINMA are only permitted to send cryptocurrencies or other tokens to **external wallets belonging to their own customers whose identity has already been verified** and are only allowed to receive cryptocurrencies or tokens from such customers. FINMA-supervised institutions are thus not permitted to receive tokens from customers of other institutions or to send tokens to such customers. This practice applies as long as information about the sender and recipient cannot be transmitted reliably in the respective payment system. **Unlike the FATF standard**, this established practice **applies in Switzerland without the exception for unregulated wallets** and is therefore one of the most stringent in the world."

Of course, once users receive these funds, they can transmit them to any other unregulated wallet, whether these addresses are owned by the same user or another recipient.

How Might VASPs Comply with Travel Rule Obligations?

It is up to each VASP to decide how to comply with the Travel Rule requirements. Some organizations may simply only permit non-regulated, non-VASPs to interact with their products. For others, using a third-party tool to transmit information off-chain is the most efficient and reliable method that will allow entities to comply with the Travel Rule.

Relating to the transmission of the required data, FinCEN states in their May 9, 2019 guidance that "…if a given transmission protocol is unable to accommodate such information, the obligated person may provide such information in a message different from the transmittal order itself." The FATF recommendations (updated June 2019) also state similarly that "the information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers." Therefore, on-chain sharing of information is not required. This allows the Travel Rule information-sharing process to remain separate from any transacted asset.

There may be additional work required by regulated entities to compile their data into a transmittable form and / or to use a third-party transmission protocol to send the required information to the recipient regulated institution. These challenges are not unique to transacting in any particular asset and apply to the VASP itself,

rather than any individual cryptocurrency. The VASP is the regulated entity in this case, not the cryptocurrency.

One example of a company providing this third-party information transmission service is CipherTrace with its TRISA product. However, almost any direct method of communication, such as email or file transfer, could suffice. Of course, ComplyFirst recommends that VASPs follow common messaging standards where possible.

Some cryptocurrencies allow for “memo” or other extra fields to include arbitrary information, which could be used to send information necessary to fulfill the Funds Travel Rule requirements. ComplyFirst recommends against using these protocol message transmission methods. They vary significantly by cryptocurrency, can change over time, may cost higher fees and lead to unnecessary chain bloat, and may share proprietary information on a public ledger. Building infrastructure reliant on protocol transmission methods is strongly ill-advised due to the changing nature of many cryptocurrency protocols. Services should invest in standardizing entity-to-entity secure solutions for off-chain information exchange rather than building small silos for individual assets. Furthermore, the consequences of encryption error are lower for direct lines of communication than for information stored on a public ledger.

However information is shared, services should remain aware of other relevant privacy regulations, including GDPR. Encryption alone may not be sufficient to comply with certain privacy and data protection regulations. Running afoul of these could expose services to legal liability.

Does the Funds Travel Rule apply to all cryptocurrencies?

Yes, VASPs must meet the Funds Travel Rule requirements for all cryptocurrencies. FinCEN’s May 9, 2019 guidance reminds VASPs (likely including cryptocurrency exchanges) of their obligations to comply with BSA regulations. The Funds Travel Rule is a BSA regulation. Other jurisdictions have similar regulations.

It would appear to be inappropriate to state that any cryptocurrency is compliant or not compliant with the Funds Travel Rule, since the Funds Travel Rule appears to apply to regulated entities, rather than the underlying assets in which the entities trade.

FinCEN’s May 9, 2019 guidance states that "A money transmitter that operates in anonymity-enhanced CVCs for its own account or for the accounts of others (regardless of the frequency) is subject to the same regulatory obligations as when operating in currency, funds, or non-anonymized CVCs." Therefore, it doesn’t appear that regulated entities would need to treat anonymity-enhanced CVCs differently from a regulatory compliance perspective than non-anonymized CVCs, like Bitcoin.

The guidance then goes on to state "In other words, a money transmitter cannot avoid its regulatory obligations because it chooses to provide money transmission services using anonymity-enhanced CVC". This appears to further reiterate that VASPs aren't prohibited from transmitting or receiving anonymity-enhanced CVCs.

A logical conclusion would be that from the regulatory compliance perspective, transmitting funds denominated in an anonymity-enhanced CVC would be equivalent to transmitting funds denominated in a non-anonymized CVC like Bitcoin.

Conclusion

The Travel Rule is a burden to share information placed on VASPs, not on any cryptocurrency protocol itself or non-VASPs who use cryptocurrencies. Individuals and entities must determine for themselves if they are a VASP or not. ComplyFirst generally recommends that VASPs share information off-chain using a direct line of communication or a third-party tool. We do not recommend using cryptocurrency protocol features to transmit this information.

There appear to be no Travel Rule regulations specific to any particular asset. Thus, VASPs must meet these requirements for any asset. Since information may be shared off-chain, there does not appear to be any compliance or technical reason why certain assets cannot be included in a proper Funds Travel Rule compliance program.

Further Reading

- Perkins Coie Whitepaper: https://www.perkinscoie.com/en/news-insights/anti-money-laundering-regulation-of-privacy-enabling-cryptocurrencies.html
- FinCEN May 2019 Guidance: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf
- FATF Recommendations: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
- Switzerland FINMA Guidance: https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/
- Monero Compliance Workgroup: https://web.getmonero.org/2019/12/05/funds-travel-rule.html
- Coin Center: https://www.coincenter.org/the-upcoming-fatf-interpretive-note-is-not-doomsday-for-cryptocurrency/
- Coin Center: https://www.coincenter.org/are-regulators-poised-to-demand-cryptocurrency-address-whitelisting-probably-not/
- Electric Coin Company: https://z.cash/compliance/
- Electric Coin Company: https://electriccoin.co/blog/how-zcash-is-compliant-with-the-fatf-recommendations/

ComplyFirst

ABOUT COMPLYFIRST

This report reflects an independent analysis by ComplyFirst and is intended as a tool to help law enforcement, regulators and industry participants understand and evaluate information that may be relevant to AML compliance. ***The report does not reflect a legal conclusion and is no indication of qualitative value of an asset or suitability for investment or any other purpose and is solely for use by ComplyFirst and not for reliance by any other party.***

ComplyFirst's analytical framework is based on relevant federal law, including FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001). Neither the report nor our framework constitute an exhaustive treatment of the legal and regulatory issues relevant to conducting an analysis of AML compliance and ComplyFirst does not analyze other laws or regulations which may apply. The analysis concerning AML compliance may evolve over time as the nature of digital assets, applicable precedent and FinCEN statements and interpretations change and evolve. ComplyFirst's framework has not been endorsed by FinCEN or any other government authority.

The report is based on a limited review of factual information publicly available or otherwise made available to ComplyFirst. Not all potentially relevant factual information has necessarily been reviewed and no independent investigation or analysis, apart from ComplyFirst's own efforts, has been taken to confirm information on which this analysis is based. We do not assume any responsibility for the completeness of the information upon which our analysis and determination is based. It is possible that if additional facts where known or assumed or understood facts prove to be incorrect, the analysis would be materially different.

ComplyFirst

DOCUMENT HISTORY

Date	Description
11/20/2020	Initial public release
12/7/2020	Terminology changes