Updates
November 07, 2023
Treasury Proposes Broad Reporting Requirements for Cryptocurrency Mixing Transactions—Implications for Financial Institutions

The U.S. Department of the Treasury (Treasury), through its Financial Crimes Enforcement Network (FinCEN), proposed on October 19, 2023, to apply the authorities in Section 311 of the USA PATRIOT Act to impose requirements on financial institutions that engage in convertible virtual currency (CVC) transactions with CVC mixers. The proposed rule, if adopted, would require covered financial institutions to report to FinCEN any CVC transactions they process that (1) involve "CVC mixing" and (2) have a nexus to a foreign jurisdiction.

Treasury believes that imposing this reporting requirement would: (1) deter certain customer behaviors pertaining to the use of CVC mixers, (2) provide law enforcement with valuable information to combat illicit finance relying on autonomy created by mixers, and (3) shine light on—and provide transparency to—state-sponsored and state-affiliated illicit activity, including weapons of mass destruction (WMD) proliferation financing.

Importantly, the term "CVC mixing" covers more than just transactions that involve CVC mixers like Tornado Cash. The proposed rule defines the term to seemingly encompass CVC transactions that involve technologies, services, or methods that *have the effect* of obfuscating the source, destination, or amount of a CVC transaction, regardless of whether the obfuscation was intentional.

While this is currently a proposed rule, it provides valuable insight into the Treasury's view of risks associated with CVC mixing. All U.S. financial institutions with CVC exposure should take this information and any potential new requirements into account in relation to their Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) program and risk management framework. Comments regarding this rule will be accepted by the Treasury through January 22, 2024.

Background

In the proposed rule, FinCEN defines CVC mixing as the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more CVC transactions. The Treasury has indicated that because CVC mixing is intended to make the underlying transactions untraceable and anonymous, this activity is ripe for abuse by—and is frequently used by—illicit foreign actors that threaten the U.S. financial system and U.S. national security. On the other hand, privacy advocates support CVC mixing as a legitimate exercise to maintain transactional and personal privacy on the public blockchain, especially in certain repressive jurisdictions.

Over the years, the Treasury and the U.S. Department of Justice (DOJ) have taken significant actions against certain CVC mixers that were intimately involved in illicit finance, and Treasury, acting through its Office of Foreign Asset Control (OFAC), imposed sanctions on certain CVC mixers.[1] Moreover, in its *Illicit Finance Risk Assessment of Decentralized Finance*, Treasury recently highlighted how criminals use CVC mixers to functionally obfuscate the source, destination, or amount involved in a cryptocurrency transaction and how these activities presented significant money laundering risks in the area of decentralized finance.

Section 311 has typically been used over the years to designate and impose restrictions on certain foreign financial institutions and countries, although it has been applied by Treasury previously in the context of CVC against cryptocurrency exchange/transfer services Bitzlato and Liberty Reserve.[2] However, this proposed rule represents the first time the Treasury has sought to usea Section 311 designation and ruling to cover a class of transactions.

The proposed rule is directed to "covered financial institutions," which encompasses all financial institutions covered under the BSA, including banks, broker-dealers, money services businesses (MSBs), mutual funds, and commodity futures merchants and introducing brokers in commodities, among many others. The rule, however, will have the most significant impact on CVC exchanges (which are MSBs) and other types of financial institutions, including banks and trust companies engaged in custody activities that are directly involved in CVC transactions on behalf of customers.

If adopted, the rule would require covered financial institutions to conduct blockchain analytics using public or private tools to identify covered transactions involving CVC mixing activity with a foreign nexus and report to FinCEN within the proposed 30-day period. FinCEN expects that covered financial institutions would use a risk-based approach to comply with the rule, including by using the blockchain analytic tools commonly available to identify covered transactions. However, under the proposal, all covered transactions identified must be reported, and failures to comply could result in civil or criminal penalties under the enforcement provisions of the BSA.

Section 311 of the USA PATRIOT Act: Application to CVC Mixing Activity

Section 311 of the USA PATRIOT Act grants the secretary of the Treasury (Secretary) the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transaction, or type of account is of "primary money laundering concern," to require domestic financial institutions and financial agencies to take certain "special measures" against the entity. Section 311 of the USA PATRIOT Act

provides the Secretary with a range of options that can be adapted to target specific money laundering and terrorist financing risks. The following special measures can be imposed individually, jointly, in any combination, and in any sequence:

- Recordkeeping and reporting certain transactions.
- Collection of information relating to beneficial ownership.
- Collection of information relating to certain payable-through accounts.
- Collection of information relating to certain correspondent accounts.
- Prohibition or conditions on the opening or maintenance of correspondent or payable-through accounts.

There are several steps the Secretary must address prior to issuing a Section 311 rule. Before making a finding that reasonable grounds exist for concluding that a class of transactions is of primary money laundering concern, the Secretary is required to consult with the secretary of state and the attorney general and must consider various factors set out in the statute, including: (1) the extent to which such class of transactions is used to facilitate or promote money laundering; (2) the extent to which such class of transactions is used for legitimate business purposes; and (3) the extent to which such action is sufficient to ensure the purposes of Section 311 are fulfilled and to guard against international money laundering and other financial crimes.

In this proposed rule, FinCEN identifies and works through each of the requirements in the statute and justifies the action against CVC mixing based on, among other things, compelling national security concerns. FinCEN explains that in recent years, North Korea has relied on CVC mixing in laundering the proceeds of its cyber heists to finance its WMD program. FinCEN further notes that CVC mixing activity is associated with the top 10 most common ransomware variants reported in suspicious activity report (SAR) data, including several Russian-affiliated variants.

At this juncture, FinCEN has issued a Notice of Proposed Rule Making (NPRM) setting out the justifications for the designation under Section 311 and the proposed special measures to be taken—in this case, imposition of reporting and record-keeping requirements. This is a regulatory process and is subject to a public notice and comment period that ends January 22, 2024. Once the comment period closes, FinCEN may issue a final rule in the form proposed or with amendments based on the commentary received.

Proposed Reporting and Record-keeping Requirements

FinCEN proposes that covered financial institutions would be required to report when their customers send or receive CVC transactions with indicia of CVC mixing. As previously noted, FinCEN explicitly expects covered financial institutions to employ a risk-based approach to compliance, including by using the free and paid blockchain analytic tools that are commonly available. Notably, FinCEN would not expect covered financial institutions to conduct lookbacks addressing conduct prior to the issuance of the final rule.

The following are the types of information that the rulemaking proposes to collect pertaining to CVC mixing transactions: (1) amount of any CVC transferred, in both CVC and its U.S. dollar equivalent when the transaction was initiated; (2) CVC type; (3) CVC mixer, if known; (4) CVC wallet address associated with the mixer and the customer; (5) transaction hash; (6) date of transaction; (7) internet protocol (IP) address and time stamps associated with the transaction; and (8) narrative.

The following are the types of information that the rulemaking proposes to collect pertaining to the customers implicated in such transactions: (1) name, date of birth, and address; (2) email address associated with any and all accounts from which or to which the CVC was transferred; and (3) unique identifying number.

Questions and Ambiguities Raised by the Proposed Rule

FinCEN states that the term "CVC mixing" covers more than just transactions involving what are traditionally considered to be CVC mixers. Rather, there are various methods that CVC users—and CVC mixers—may employ to obfuscate transactions. As a result, the proposed rule defines "CVC mixing" broadly to include the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used. This would explicitly include activities such as (1) pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts; (2) using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction; (3) splitting CVC for transmittal and transmitting the CVC through a series of independent transactions; (4) creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions; (5) exchanging among types of CVC or other digital assets; or (6) facilitating user-initiated delays in transactional activity. In addition, a "CVC mixer" would be defined as any person, group, service, code, tool, or function that facilitates CVC mixing, as broadly defined above.

A "covered transaction" subject to the record-keeping and reporting requirements under the proposed rule would include a transaction in CVC by, through, or to the covered financial institution that the covered financial institution "knows, suspects, or has reason to suspect" involves CVC mixing within or involving a jurisdiction outside the United States. FinCEN notes that limiting the rule to transactions "in CVC" means that the reporting obligations under this special measure apply to covered financial institutions that directly engage with CVC transactions, such as a CVC exchange. It also means that covered transactions would not include transactions that are only indirectly related to CVC, such as when a CVC exchanger sends the non-CVC proceeds of a sale of CVC that was previously processed through a CVC mixer from the CVC exchanger's bank account to the bank account of the customer selling the CVC. Notwithstanding these limitations, the language "by, through, or to" the covered financial institution is very broad, and the "indirect exposure to mixing" could complicate these determinations in situations in which the mixing activities occurred several transactions or hops before or after the covered financial institution touched it. Impacted covered financial institutions will need to thoroughly analyze their systems and processes to ensure that there are no gaps in coverage relating to the identification of these transactions.

The expansive definition of CVC mixing creates some uncertainties about what is and is not covered by the term. For instance, while FinCEN's summary of the proposed rule highlights that "CVC mixing is intended to make CVC transactions anonymous," the ultimate definition used in the proposed rule does not contain an intent requirement. Rather, under the proposed rule, "CVC mixing" is the "facilitation of CVC transactions *in a manner* that obfuscates the source, destination, or amount involved in one or more transactions." Indeed, the examples identified in *the proposed rule's* definition of CVC mixing seem to sweep in features of the blockchain ecosystem that have not *historically* been considered CVC mixing:

1. **Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts.** This category of CVC mixing would seem to capture centralized exchanges that often use pooled wallets to facilitate

trading on the exchange. FinCEN also indicates that this category is intended to cover the pooling of CVC from multiple persons into a smart contract.

2. **Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction.** This broad definition may capture oracles, forms of staking, and well-intentioned forms of vesting lockups or programmatic releases by issuers. Many issuers impose time delays on delivery of tokens, and these may be captured in this definition.
3. **Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions.** Splitting CVC for transmittal is a common activity. It is common for two parties who have not transacted before to conduct small test transactions before transferring larger amounts. Even if not conducting initial test transactions, participants may split up major transfers to avoid risk created by the irrevocable nature of blockchain transactions. All of these could be included in this definition.
4. **Creating and using single-use wallets, addresses, or accounts and sending CVC through such wallets, addresses, or accounts through a series of independent transactions.** There are many reasons users may want to create a single-use wallet, including for risk management. This practice is important to addressing security concerns that are important to many blockchain users.
5. **Exchanging between types of CVC or other digital assets.** The fungible nature of CVC and the proliferation of platforms and assets leads CVC exchange to be a common occurrence. It is not uncommon to conduct an exchange between assets to obtain another form of CVC that will be accepted by a counterparty. One technical advantage of smart contracts is that they can execute many of these transactions programmatically, which is flagged above in item (2).
6. **Facilitating user-initiated delays in transactional activity.** As mentioned above, commercial parties may engage in user-initiated delays for commercial, practical, or risk-based reasons. These could include prearranged delivery schedules of tokens sold by projects, a choice to avoid fees, or preferences for timing of payments, like scheduling a bill payment.

In each of these cases, ambiguities exist in FinCEN's expansive proposed definition of CVC mixing that, if adopted, will lead to overbroad record-keeping and reporting requirements. From a practical perspective, the ambiguities will likely significantly diminish access to the types of transactions implicated, even where such transactions do not raise significant national security concerns.

It bears noting that to avoid imposing additional undue burdens, FinCEN specifically excepts the use of internal protocols or processes to execute transactions by banks, broker-dealers, or money services businesses, including virtual asset service providers, that would otherwise constitute CVC mixing, provided these financial institutions preserve records of the source and destination of CVC transactions when using such internal protocols. However, because of the definition of those terms elsewhere in the BSA, the exception would seemingly only apply to banks, broker-dealers, or money services businesses subject to U.S. jurisdiction. Thus, transactions with a foreign CVC exchange that operates exclusively outside the United States would seemingly not qualify for the exception because the exchange would not fit within the BSA's definition of a money services business.

Questions for Public Comment

FinCEN invites comments on the proposed rule concerning the following areas:

- CVC mixing as a class of transactions of primary money laundering control.
- The proposed definitions.
- Alternative special measures that may be appropriate.

- Recordkeeping and reporting.
- Burden and other impacts of the proposed rule.

Each of these areas contains a series of more specific questions for consideration. Comments are due January 22, 2024.

Key Takeaways

All financial institutions with CVC exposures should consider the following:

1. Review the proposal and consider providing responses to FinCEN to the questions, as this will help inform and provide guidance to FinCEN concerning these proposed processes.
2. Certain financial institutions with CVC exposures may need to select, obtain, and understand more sophisticated blockchain analytic tools to enable the identification of covered transactions, begin developing policies and procedures relating to the expected information, and report processes that will be included in any final rule.
3. Financial institutions that are proficient with blockchain analytics tools may review prior transactions over a specified time period to identify those that may have involved CVC mixers and other manners of obfuscation (e.g., peel chains, chain hopping, etc.) to understand the scope and extent of reporting that may be required and consider taking steps to reduce these exposures.
4. Potential information gaps should also be considered to ensure that any transactions "by, through, or to" a financial institution can be identified.
5. Issuers of CVC wallets and other entities subject to the exception should consider the records requirements in the proposal and the manner in which they will be satisfied to ensure that the exception is applicable.
6. Policies and procedures relating to blockchain analytics and processes pertaining to the identification of covered transactions will be a critical component, as well as information collection and reporting processes that will need to be developed.

For matters related to CVC mixers and this Section 311 proposal financial institutions, consult with experienced counsel.

Endnotes

[1] Perkins Coie Client Alert, OFAC Takes Action Against Virtual Currency Tornado Cash in Novel Application of Sanctions Authorities | Virtual Currency Report; DOJ, Tornado Cash Founders Charged with Money Laundering and Sanctions Violations, Aug. 23, 2023; OFAC, Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash, Aug. 23, 2023.

[2] In Bizlato, FinCEN analyzed the Section 311 special measures through section 9714 of the Combatting Russian Money Laundering Act (P.L 116-283 as amended by P.L. 117-81) and determined that the special measures would not address the risks and used other measures under section 9714. A comprehensive list of all FinCEN section 311 actions can be found on FinCEN's webpage at: 311 and 9714 Special Measures | FinCEN.gov.

Authors

Explore more in

White Collar & Investigations International Trade Fintech & Payments

Related insights

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors

Update

January Tip of the Month: Trump Executive Orders Challenge DEI Programs