October 23, 2023

FinCEN Announces Notice of Proposed Rulemaking on CVC Mixing

FinCEN Proposes Rule to Enhance Transparency in CVC Mixing and Combat Terrorist Financing

SUMMARY

On October 19, 2023, the United States Department of the Treasury ("Treasury") Financial Crimes Enforcement Network ("FinCEN") issued a Notice of Proposed Rulemaking ("Proposal") that would identify Convertible Virtual Currency ("CVC") mixing as a class of transactions of primary money laundering concern and require covered financial institutions to implement recordkeeping and reporting requirements in relation to CVC mixing transactions.[1] CVC refers to virtual currency[2] that either has an equivalent value as currency or acts as a substitute for currency and is therefore a type of "value that substitutes for currency." The Proposal would apply to transactions in CVC, *i.e.*, when a covered financial institution engages directly with CVC, and not to transactions only indirectly related to CVC.

The Proposal follows prior actions by Treasury to target illicit financial activity involving CVC mixing services and is intended to support Treasury's continued efforts to promote transparency for such activities, to enable law enforcement and regulators to support money laundering investigations, and to deter the illicit use of CVC mixing services. It would require covered financial institutions to report information about a transaction, in the manner prescribed by FinCEN, when the institution knows, suspects, or has reason to suspect it involves CVC mixing within or involving jurisdictions outside the United States, and to maintain records related to such transactions.

Over the past few weeks, terror financing and other forms of illicit financial activity have received increased public, political and regulatory attention following the Hamas terrorist attacks in Israel. The Proposal cites not only the increased use of CVC mixing services, but also the use of CVCs in terror finance, including to fund Hamas. Moreover, on October 20, 2023, FinCEN issued an alert to financial institutions to counter

financing to Hamas and its terrorist activities, noting that virtual currency is one of the ways that Hamas finances its activities and some of the identified red flags involve virtual currency.[3] The alert is intended to assist financial institutions in identifying funding streams for Hamas, including by highlighting red flags to help detect, prevent, and report potential suspicious financial activity relating to Hamas. FinCEN urges financial institutions to be vigilant in identifying suspicious activity relating to Hamas and reporting to FinCEN.

BACKGROUND

Section 311 of the USA PATRIOT Act grants the Secretary of the Treasury authority,[4] which has been delegated to the Director of FinCEN, to require domestic financial institutions and domestic financial agencies to take certain "special measures"[5] upon finding that reasonable grounds exist for concluding that one or more classes of transactions within or involving a jurisdiction outside of the United States is of primary money laundering concern.

A. CONVERTIBLE VIRTUAL CURRENCY MIXING

The public nature of most CVC blockchains provides a permanent, recorded history of all previous transactions on the blockchain. As a means to protect the anonymity of blockchain users in their financial transactions, tools such as CVC mixers provide a service[6] whereby they receive cryptocurrencies from users and act as intermediaries in sending corresponding amounts to the recipients' addresses in order to shield the origins, destinations, and/or amounts of particular transactions.[7]

There are a number of methods by which CVC mixing services can seek to protect the anonymity of blockchain users, including:

- pooling or aggregating CVC by combining CVC from multiple persons, wallets, addresses or accounts, which makes it more difficult to identify persons associated with each transaction;
- splitting CVC transactions into multiple smaller transmittals to make the transactions blend in with each other;
- using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction to hide individual transaction details;
- creating and using single-use wallets, addresses, or accounts and sending CVC through them in a series of transactions, often referred to as "peel chain";
- exchanging between types of CVC, or other digital assets, often referred to as "chain hopping"; and
- using software that can delay transactions and thus make the connection between inputs and outputs harder to determine.

B. USE OF CVC MIXING BY ILLICIT FOREIGN ACTORS

In the Proposal announced on October 19, FinCEN describes how CVC mixing is vulnerable to abuse and misuse.[8]

For example, it notes that various actors, including foreign entities, are increasingly using CVC mixing in ways that threaten U.S. national security and the integrity of the financial system.[9] FinCEN notes that the Democratic People's Republic of Korea ("North Korea" or the "DPRK") has used CVC mixing to evade international sanctions and finance its weapons of mass destruction ("WMD") program. In 2022, the DPRK-controlled Lazarus Group carried out the Axe Infinity Ronin Bridge heist, which involved the theft of almost $620 million and remains the largest cyber heist to date. In doing so, the Lazarus Group used at least two CVC mixers to launder the proceeds of the theft.[10] In addition, FinCEN states that Russian ransomware actors and buyers and sellers on Russian darknet markets have employed CVC mixing activities to facilitate illicit activity.[11] The Proposal notes that CVC mixing services rarely, if ever, provide the resulting transactional chain or information collected as part of these transactions to regulators or law enforcement.[12]

CVC MIXING AS A PRIMARY MONEY LAUNDERING CONCERN

The Proposal sets forth FinCEN's finding that reasonable grounds exist for concluding that transactions involving CVC mixing within or involving a jurisdiction outside the United States are a class of transactions that is of primary money laundering concern.[13] In particular, the Proposal discusses FinCEN's findings with respect to the requisite statutory factors: (1) the extent to which the class of transactions is used to facilitate or promote money laundering in or through a jurisdiction outside of the United States, including money laundering activity with connections to international terrorism, organized crime, and proliferation of WMDs and missiles; (2) the extent to which a class of transactions is used for legitimate business purposes; and (3) the extent to which action by FinCEN would guard against international money laundering and other financial crimes.[14]

In considering the first factor, FinCEN highlights the below considerations:

- **International character of CVC mixing transactions**: FinCEN notes that CVC mixers frequently operate in or deal with countries outside the United States and employ methods to hide their operations. FinCEN highlights that no CVC mixers are currently registered with FinCEN.[15]
- **Laundering from large-scale CVC theft and heists**: FinCEN also notes that CVC mixers have been used to launder money from large-scale CVC thefts, including in the aforementioned example involving the North Korean government.[16]
- **Ransomware and darknet markets**: The Proposal asserts that cybercriminals, particularly those deploying ransomware, use CVC mixers to obscure the origins of their illicit gains. FinCEN highlights that between January 2021 and June 2021, the top 10 most common ransomware variants, including several Russian-affiliated variants, funneled roughly $35.2 million to CVC mixers. In addition, Hydra, a former Russian darknet marketplace that made up approximately 80% of all darknet market CVC transactions in 2021, used CVC mixers before its shutdown by U.S. and German law enforcement agencies.[17]

With respect to the second factor (the extent to which the class of transactions is used for legitimate business purposes), FinCEN acknowledges that there are legitimate reasons why responsible actors might

want to transact privately using CVC mixers, but nevertheless concludes that these transactions are of primary money laundering concern due, in part, to the difficulty in assessing the extent of legitimate use.[18]

Addressing the third factor (the extent to which action by FinCEN would guard against international money laundering and other financial crimes), FinCEN notes that the proposed recordkeeping and reporting requirements would guard against international money laundering and other financial crimes by increasing transparency in these transactions, thus rendering them less attractive to illicit actors, while also providing additional information to support law enforcement investigations.

PROPOSED RECORDKEEPING AND REPORTING REQUIREMENT

Section 311 of the USA PATRIOT Act provides that upon making the above findings and engaging in the requisite consultations, FinCEN may impose one or more of the "special measures" set out in the Act. Through "special measure one," FinCEN may require domestic financial institutions and domestic financial agencies to maintain records, file reports, or both, concerning the aggregate amount of transactions or individual transactions.[19]

FinCEN proposes to require covered financial institutions to implement certain recordkeeping and reporting requirements related to CVC mixing transactions and uses certain existing regulations to define the scope of entities and transactions covered by the Proposal. The term "covered financial institution" includes any financial institution defined in 31 C.F.R. § 1010.100(t), which includes, among others, banks, money services businesses, brokers or dealers in securities, futures commission merchants and introducing brokers in commodities registered with the Commodity Futures Trading Commission, and mutual funds. The Proposal does not expand this definition. A "covered transaction" under the Proposal means a transaction as defined in 31 C.F.R. § 1010.100(bbb)(1) in CVC, that is carried out "by, through, or to the covered financial institution," and "that the covered financial institution knows, suspects, or has reason to suspect involves CVC mixing within or involving a jurisdiction outside the United States."[20] This definition captures a wide range of transactions covered by 31 C.F.R. § 1010.100(bbb)(1), but importantly is limited to transactions in CVC, which means the Proposal will capture covered financial institutions that are directly involved in CVC transactions, but not transactions that are only indirectly related to CVC.[21] As an example, the Proposal explained that by limiting covered transactions to those in CVC, it 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 CVC."[22]

In connection with covered transactions, FinCEN proposes to require covered financial institutions to collect and report the following information:

- amount of any CVC transferred, in both CVC and its U.S. dollar equivalent, when the transaction was initiated;

- CVC type used in a covered transaction;
- CVC mixer used, if known;
- CVC wallet address associated with the mixer;
- CVC wallet address associated with the customer;
- transaction hash;
- date of transaction;
- IP addresses and time stamps associated with the covered transaction; and
- a description of activity observed by the covered financial institution.[23]

The Proposal also would require covered institutions to collect and report information about the customer associated with the covered transaction, including the customer's full name, date of birth, address, email address, and unique identifying number, such as the customer's Taxpayer Identification Number ("TIN").[24] The reports required by the Proposal would be in addition to, rather than instead of, any obligation of a covered financial institution to file a Suspicious Activity Report (SAR).[25]

The Proposal would require a covered financial institution to collect, maintain records of, and report to FinCEN within 30 calendar days of initial detection of a covered transaction. FinCEN notes that the Proposal only would require a covered financial institution to report information in its possession, and would not require it to reach out to the transactional counterparty to collect additional information. The Proposal also would not require covered financial institutions to look back to transactions that occurred prior to the issuance of a final rule.[26] The Proposal would also require covered financial institutions to maintain any records documenting compliance with the requirements of the new regulation.[27]

FinCEN notes in the Proposal that it expects covered financial institutions to employ risk-based approaches to compliance with the Proposal, and more broadly, the Bank Secrecy Act, and mentions various free and paid blockchain analytic tools commonly available to monitor and detect risks.[28]

FinCEN invited comments on a number of specific questions, including as to the impact of the Proposal on legitimate financial activities and on blockchain privacy or pseudonymity, challenges in identifying the foreign nexus of a CVC mixing transaction, the scope of recordkeeping requirements, the list of information to be collected and reported, and, in cases where the customer of the covered financial institution is a legal entity, whether beneficial ownership of the legal entity should also be reported.[29]

OBSERVATIONS AND IMPLICATIONS

The Proposal marks the first time that FinCEN has used its authority under Section 311 of the USA Patriot Act to target a class of transactions as of primary money laundering concern. FinCEN has rarely invoked "special measure one". This is the latest in a series of actions by Treasury to target illicit financial activity that involves virtual currency and CVC mixing, and the press release issued in connection with the Proposal

notes that it is a key part of these efforts.[30] While the Proposal recognizes that there are certain legitimate reasons for seeking additional privacy and security in conducting financial transactions—such as when one or more parties live in a repressive regime—these proposed requirements underscore that FinCEN and other U.S. regulators view the increased anonymity provided by CVC mixers with considerable skepticism and as a significant money laundering risk. It is likely that FinCEN and other regulators will seek to ensure that, as part of their BSA/AML compliance programs, covered financial institutions incorporate monitoring, controls, and other safeguards designed specifically to detect and report illicit activity involving CVC mixing and/or other anonymity-enhancing tools in the digital assets sphere.

Although the Proposal would apply to and affect banks and money services businesses that transact in CVCs, it would also apply to other entities that fall within the definition of a covered financial institution and often have more direct involvement in, or exposures to, digital assets—such as broker-dealers, futures commission merchants and introducing brokers in commodities registered with the Commodity Futures Trading Commission, and mutual funds. For this reason, trading firms, investment firms, and other entities that operate in the digital assets space and fall within the definition of a covered financial institution would be required to meet the same collection, reporting, and recordkeeping obligations as banks when designing and executing their Bank Secrecy Act/anti-money laundering compliance programs. In addition, because these entities often have more direct exposure to transactions involving digital assets (including CVC), they would in some instances likely maintain access to, and therefore have an obligation to collect and report, a wider range of information about CVC transactions (and the parties involved) than banks. Finally, individuals and entities that are not covered financial institutions but participate in CVC transactions would face indirect effects from implementation of the Proposal, insofar as certain information they provide to covered financial institutions in the course of a CVC transaction may be reported to FinCEN, which could lead to inquiries from FinCEN or other law enforcement agencies.

In addition, and as noted above, this Proposal comes at a time when there is heightened public and political attention on terror financing. Congressional leaders from both parties have expressed concern about the dangers posed by terrorist financing through CVC following reports of Hamas fundraising efforts leading up to the recent attacks.[31] FinCEN's press release in connection with the Proposal notes that "[t]his increased transparency is also consistent with longstanding Treasury Department efforts to counter the efforts of terrorist groups, such as Hamas and Palestinian Islamic Jihad, that engage in violence against innocent civilians; the efforts of ransomware criminals targeting critical infrastructure; and the efforts by state actors and their supporters to evade U.S. and global sanctions."[32] Also in support of these efforts, on October 18, 2023, the Treasury's Office of Foreign Assets Control imposed sanctions on certain Hamas terrorist group members,[33] and, as noted above, FinCEN issued an alert to financial institutions to counter financing to Hamas and its terrorist activities on October 20, 2023. Covered financial institutions should closely monitor this Proposal and other efforts by regulators to increase transparency and limit anonymity in the digital assets space due to concerns about money laundering and other illicit financial activity.

The Proposal will be subject to a 90-day comment period that ends on January 22, 2024.

* * *

ENDNOTES

1 FinCEN, Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern (Oct. 19, 2023), *available at* https://www.fincen.gov/sites/default/files/federal_register_notices/2023-10-19/FinCEN_311MixingNPRM_FINAL.pdf.

2 The term "virtual currency" refers to a medium of exchange that can operate like currency, "including [any] 'digital currency,' 'cryptocurrency,' 'cryptoasset,' and 'digital asset,'" but does not have all the attributes of "real," or fiat, currency; *see* Proposal at 7.

3 FinCEN, Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities (Oct. 20, 2023), *available* at https://www.fincen.gov/news/news-releases/fincen-alert-financial-institutions-counter-financing-hamas-and-its-terrorist.

4 *See* Pub. L. No 107-56, § 311, 115 Stat. 272, 402 (2001) (codified at 31 U.S.C. § 5318A).

5 Pursuant to Treasury Order 180-01 (Jan. 14, 2020), the authority of the Secretary to administer the BSA, including, but not limited to, 31 U.S.C. § 5318A, has been delegated to the Director of FinCEN; *see* Proposal at 2, footnote 2.

6 The term "CVC mixing" is defined in the Proposal as 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, such as: (A) Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts; (B) Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction; (C) Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions; (D) Creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions; (E) Exchanging between types of CVC or other digital assets; or (F) Facilitating user-initiated delays in transactional activity. The Proposal notes that notwithstanding the foregoing, CVC mixing does not include 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 that these financial institutions preserve records of the source and destination of CVC transactions when using such internal protocols and processes; and provide such records to regulators and law enforcement, where required by law. *See* Proposal at 75 – 76.

7 *Id*. at 7.

8 *Id*. at 5.

9 *Id*. at 6.

10 *Id*. at 15.

11 *Id*.

12 *Id*. at 7 – 10.

13 *Id*. at 10.

14 *Id*. at 13.

15 *Id*. at 14 – 15.

16 *Id*. at 16 – 18.

17 *Id*. at 12, 18 – 20.

18 *Id*. at 22.

19 *Id*. at 23.

20 *Id*. at 32 – 33.

ENDNOTES (CONTINUED)

21 *Id*. at 33.

22 *Id.* at 32; *see id.* at 23.

23 *Id*. at 35 – 37.

24 *Id*. at 37 – 38.

25 *Id*. at 37.

26 *Id*. at 33.

27 *Id*. at 38 – 39.

28 *Id*. at 33.

29 *Id.* at 39 – 42.

30 FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing, *available* at https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

31 *See* Letter from various members of the United States Congress to Brian E. Nelson, Under Secretary for Terrorism and Financial Intelligence and Jake Sullivan, National Security Advisor (Oct. 17, 2023), *available at* https://www.warren.senate.gov/imo/media/doc/2023.10.17%20Letter%20to%20Treasury%20and%20White%20House%20re%20Hamas%20crypto%20security.pdf.

32 FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing, *available at* https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

33 Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators (Oct. 18, 2023), *available at* https://home.treasury.gov/news/press-releases/jy1816.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.