

January 22, 2024

Via electronic submission: <http://www.regulations.gov>

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

Re: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72,701 (Oct. 23, 2023)

Chainalysis appreciates the opportunity to respond to the request for comments by the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") on its Proposal of Special Measure Regarding Convertible Virtual Currency Mixing.

Chainalysis is the leading provider of blockchain data and analysis. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries. Our data powers investigation, compliance, and market intelligence software that has been used to help solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely.

Chainalysis shares FinCEN's interest in combating illicit activity on blockchain networks. Chainalysis was founded with the mission of building trust in blockchains, and in this response, we bring the perspective of a company that has spent the past nine years working closely with the public and private sector in an effort to understand the scope and nature of illicit activity on blockchains and support processes designed to assist its customers in mitigating that activity as much as possible.

We also bring the perspective of a company that will be directly impacted by the proposed special measures. Financial institutions leverage data and software tools provided by Chainalysis as part of their processes to comply with anti-money laundering regulations implemented and overseen by FinCEN. If the proposed regulation is adopted, Chainalysis will play a central role in providing responsive data and creating new processes to help support our customers in their efforts to comply with the recordkeeping and reporting special measures.

With this context, we strongly support FinCEN's efforts to address the unique illicit activity risks associated with convertible virtual currency (CVC) mixers, although we recommend that FinCEN consider alternatives paths than those proposed in the Notice of Proposed Rulemaking (NPRM).

Executive Summary

Chainalysis has been tracking and publishing research on illicit activity involving CVC mixers for several years. As a general matter, our data supports FinCEN's findings that CVC mixers are associated with elevated levels of illicit activity.¹ As such, we understand the basis for FinCEN's determination that transactions involving CVC mixers should be subject to heightened regulatory scrutiny.

However, we believe that the proposed special measures are too broad to effectively mitigate the illicit finance risks of CVC mixers and should be reconsidered for the following reasons:

- First, as currently drafted, the proposed special measures will be difficult to implement at scale and will result in inconsistent and excessive reporting on transactions, most of which will have no meaningful association to illicit activity.
- Second, there is an insufficient basis to conclude that the special measures will be effective in deterring bad actors from leveraging CVC mixers for illicit activities.
- Third, a deeper investment in blockchain analysis solutions offers a more effective and less resource-intensive means for understanding and mitigating the illicit finance risks associated with CVC mixers.

Chainalysis recommends that FinCEN revise the special measures to narrow the definitions in the proposal to more clearly delineate what constitutes mixing activity. Moreover, Chainalysis recommends that FinCEN research the possibility of leveraging blockchain analysis will allow it to obtain more granular insights on the intersection of mixing transactions and illicit activity.

¹ As discussed in more detail later in the submission, Chainalysis data is based on identifying services commonly understood as mixers and does not necessarily capture all activity under the broad definition of CVC mixing in the NPRM.

Comments on the Proposed Special Measures

I. Chainalysis Data on CVC Mixers

Chainalysis data supports FinCEN's findings that CVC mixers are associated with heightened levels of illicit activity. When compared with other types of blockchain-based services, CVC mixers receive a significantly larger share of funds from wallets associated with illicit activity than received by other types of services tracked by Chainalysis.

In July 2022, Chainalysis reported that almost 10% of all funds sent by addresses known to be involved in illicit activity were sent to CVC mixers.² This demonstrates a noticeable preference by certain types of bad actors to utilize CVC mixers, particularly when compared to non-illicit address types tracked by Chainalysis (e.g., centralized exchange wallet addresses, decentralized finance addresses, etc.), which send less than 0.3% of outgoing funds to mixers. At that time in 2022, the value of funds sent from illicit addresses amounted to 23% of the total value sent to CVC mixers. Notably, of the illicit wallet addresses utilizing CVC mixers, the majority were attributed to sanctioned entities, including the North Korean Lazarus Group and Russian Hydra darknet marketplace. Indeed, in Q2 2022 alone, the Lazarus Group sent over \$500 million to CVC mixers.

Chainalysis believes the outsized use of CVC mixers by foreign illicit actors demands special attention by public and private stakeholders. We support FinCEN's determination that transactions involving CVC mixers should be subject to heightened regulatory scrutiny for potential illicit activity. To that end, we stand ready to assist with our best-in-class data to help inform decisions that help prevent bad actors from leveraging CVC mixers for illicit purposes.

II. Existing processes for identifying and reporting CVC mixing

Before analyzing whether the proposed special measures will be effective, it is helpful to first understand the current way in which financial institutions are able to address potential risks associated with customer transactions involving CVC mixers.

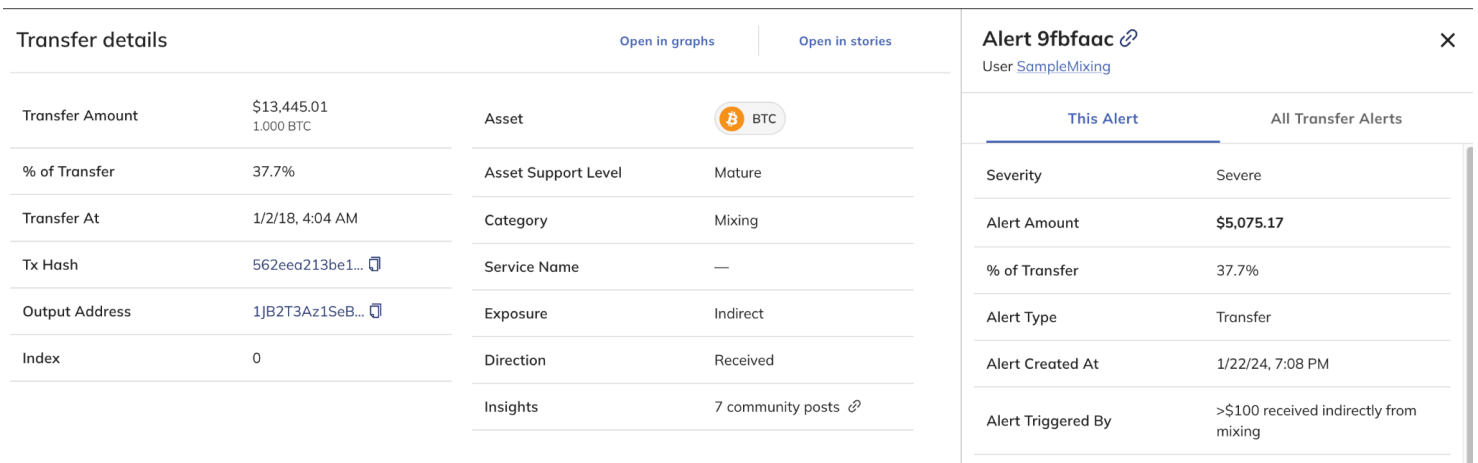
One of the central novel features of transacting on blockchains is the inherent transparency of the technology. All transactions are publicly broadcast and stored on an immutable ledger such that anyone can monitor transaction activity in real-time. However, this data is not

² Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume (July 14, 2022), Chainalysis, <https://www.chainalysis.com/blog/crypto-mixer-criminal-volume-2022/>.

easy to analyze in its raw form and lacks the context of information stored outside the blockchain network. At Chainalysis, we augment this raw data with attributions of cryptocurrency addresses to specific services and group together addresses belonging to each service or wallet in a process we call clustering.³ We then provide this augmented data to both government and private sector customers through various software tools and services designed to aid in monitoring transaction activity, investigating potentially suspicious transactions, and gaining other enhanced insights into blockchain activity.

A. Monitoring transactions involving CVC mixers

Chainalysis identifies and labels CVC mixers in our data and integrates those attributions into our products.⁴ As a result, financial institutions are able to review customer transactions in near-real time and receive information about whether those transactions involved mixing activity. The images below show an example of some of the information a financial institution can retrieve about a customer who has transacted with a CVC mixer.



The screenshot displays two panels. The left panel, titled 'Transfer details', shows transaction information for a Bitcoin transfer. The right panel, titled 'Alert 9fbfaac', provides details about a specific alert triggered by the transfer.

Transfer details		Asset	
Transfer Amount	\$13,445.01 1.000 BTC	Asset	BTC
% of Transfer	37.7%	Asset Support Level	Mature
Transfer At	1/2/18, 4:04 AM	Category	Mixing
Tx Hash	562eea213be1...	Service Name	—
Output Address	1JB2T3Az1SeB...	Exposure	Indirect
Index	0	Direction	Received
		Insights	7 community posts

Alert 9fbfaac	
Severity	Severe
Alert Amount	\$5,075.17
% of Transfer	37.7%
Alert Type	Transfer
Alert Created At	1/22/24, 7:08 PM
Alert Triggered By	>\$100 received indirectly from mixing

Image #1

³ The following blog post provides greater detail on Chainalysis makes attributions: The Data Accuracy Flywheel: How Chainalysis Consistently Identifies and Verifies Blockchain Entities (Jan. 16, 2024), Chainalysis, <https://www.chainalysis.com/blog/chainalysis-data-accuracy/>. It is important to emphasize that Chainalysis only identifies services within its data and does not attempt to identify individual blockchain users.

⁴ See Crypto Mixers and AML Compliance (Aug. 23, 2022), Chainalysis, <https://www.chainalysis.com/blog/crypto-mixers/>.

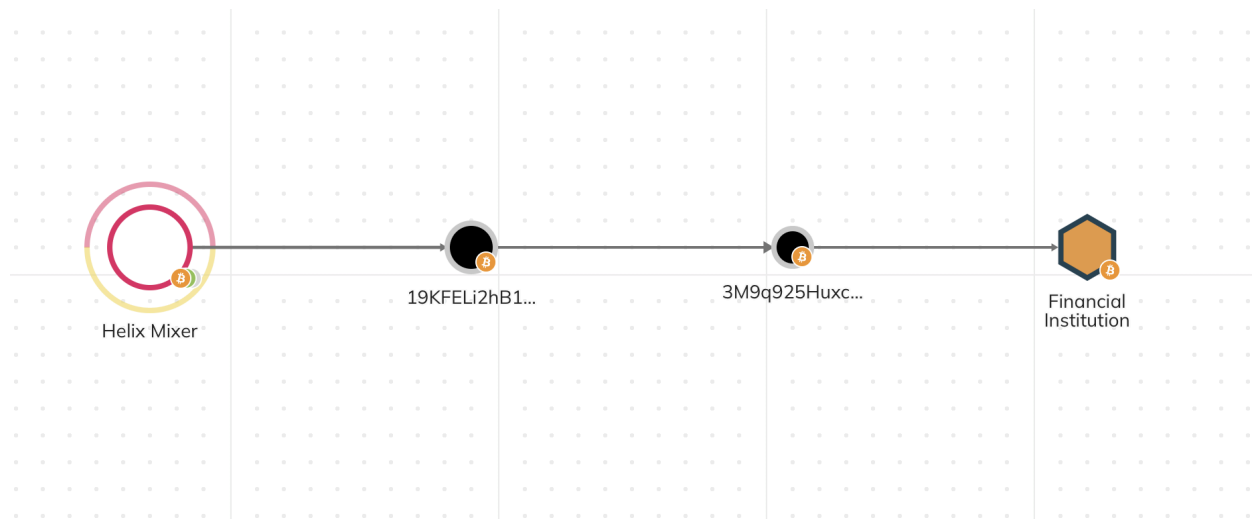


Image #2

Image #1 reflects the details of a hypothetical alert received by a financial institution. In response to this alert, compliance staff at financial institutions are able to utilize a variety of Chainalysis tools to review the transaction in more detail and gain greater insight to inform a potential response, including whether to file a Suspicious Activity Report (SAR).

The alert shows that the customer deposited 1 BTC at a financial institution and that a portion of that BTC was flagged for being associated with mixing activity. The graph in Image #2 provides more details, and shows that the BTC can be traced back to Helix Mixer, a known CVC mixer that operated on the darkweb and is identified in Chainalysis data.⁵ Chainalysis labels this transaction as having “indirect exposure” to a mixer because the funds were not sent directly from the mixer to the financial institution. It is considered indirect exposure (rather than direct exposure) because the interaction with the mixer occurred three transactions prior to the funds being sent to the wallet in consideration, as demonstrated in the graph.

As part of their BSA compliance programs, financial institutions typically implement a transaction monitoring process to automatically flag certain transactions that may involve high-risk counterparties, or otherwise have characteristics that may require investigation for suspicious activity. Our compliance solutions can provide alerts based on customized settings, such as the amount of a transaction, whether that transaction can be traced to a CVC mixer, and whether that exposure is direct or indirect.

⁵ See Chainalysis in Action: How Law Enforcement Tracked Millions’ Worth of Illicit Bitcoin in the Harmon Brothers Cases (July 26, 2023), Chainalysis, <https://www.chainalysis.com/blog/helix-mixer-harmon-brothers-investigation/>.

The above example involves a customer who deposited BTC at a financial institution that could be traced back to a mixer. However, the transparent nature of the blockchain, combined with Chainalysis software, also allows for financial institutions to track funds after they have been withdrawn from their platform. For example, a financial institution could customize their settings to send an alert if a customer were to withdraw BTC, which was then subsequently moved between several wallets before being sent to a CVC mixer.

Ultimately, there are numerous factors that may affect whether to file SAR in response to a transaction involving a mixer. Initially, a financial institution must make a risk-based decision as to whether to flag all transactions involving mixers for potential follow-up investigation or only those that meet certain parameters. Even after a financial institution receives an alert about a mixing transaction, they typically will want to analyze when the exposure to a CVC mixer occurred, how much of the transaction was associated with mixing, and how many intervening transactions occurred before or after the transaction with the financial institution. A financial institution may also analyze factors outside the specific details of a transaction, such as the jurisdiction of the customer or whether the customer has any history of interacting with a CVC mixer. Unlike in the traditional financial system, the transparency of blockchain-based systems provide a greater level of insight into the circumstances around a customer transaction, which in turn informs the SAR process.

Chainalysis also extends its transaction tracing to mixers. In other words, financial institutions can use Chainalysis tools to trace transactions through certain mixers and determine whether the source or destination of funds may be a wallet associated with illicit activity.

B. Chainalysis attribution of other non-mixing services

It is important to recognize that CVC mixers are not the only types of services that can obfuscate the source, destination, or amount involved in a CVC transaction. Even when not utilized for privacy purposes, transactions sent to or from centralized exchanges, cross-chain bridges, and DeFi protocols all complicate, to varying degrees, the otherwise straightforward ability to trace the source and recipient of a standard CVC transaction on a blockchain. Indeed, blockchain analysis is unable to trace funds through certain services.⁶

⁶ See *Why You Can't Trace Funds Through Services Using Blockchain Analysis (And Why You Don't Need to Anyway)* (Oct. 9, 2020), Chainalysis, <https://www.chainalysis.com/blog/blockchain-analysis-trace-through-service-exchange/>.

Although these services may complicate tracing, Chainalysis labels these services in our data based on their primary functions - e.g., as a service for exchanging assets, moving assets between blockchains, or conducting financial transactions - and not as “mixers.” Chainalysis reserves the designation of “mixer” for those services commonly referred to as mixers, which typically are designed and promoted for the purposes of breaking the transaction chain and obfuscating the source or destination of a transaction.

Comments on the Proposed Special Measures

- I. **The proposed special measures will be difficult to implement and will result in inconsistent and excessive reporting on transactions, most of which will have no association to illicit activity.**

Despite supporting the call for heightened scrutiny of CVC mixers, Chainalysis believes that the proposed special measures create difficult implementation issues that will hinder the goal of mitigating illicit financial activity. This is largely due to the broad scope and unclear definitions in the proposal, which would require financial institutions to submit inconsistent and unnecessary reports on transactions that have no association with illicit activity.

To briefly summarize, the NPRM, based upon a finding that CVC mixing involving jurisdictions outside the US constitutes a primary money laundering concern, FinCEN proposes imposing special measures in the form of mandatory recording and reporting requirements on all financial institutions. The proposed special measures would result in financial institutions having to identify all transactions by their customers that have a direct or indirect connection to CVC mixing activity as well as a foreign nexus. Those financial institutions would then need to maintain records and report to FinCEN on each such transaction with details about the customers involved and the nature of the transaction.

As detailed below, the proposal presents several issues that will make practical implementation difficult, inconsistent, and ineffective.

- A. The definition of CVC mixing does not include clearly articulable standards for identifying reportable transactions.

The proposal defines “CVC mixing” broadly to include any manner of facilitating a transaction that “obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used.” The proposal then cites six highly generalized examples of mixing activity, including structuring transactions into multiple smaller transactions, using single-use addresses, and exchanging between assets.

Financial institutions invariably need to review large volumes of transactions and typically rely on automated tools to assist in flagging transactions that may require further investigation or reporting to FinCEN. Therefore, it is important that a proposal for mandatory reporting clearly articulates definitions that can be integrated into tools to scalably identify reportable transactions. The current definition of CVC mixing does not lend itself to the creation of automated or consistent processes for finding reportable transactions. Instead, the definition cites numerous factors that could conceivably be interpreted to apply to countless types of transactions that seemingly have nothing to do with what is traditionally considered as CVC mixing.

Adoption of the definition of CVC mixing in the proposal would put financial institutions in the position of having to make difficult discretionary decisions about what constitutes mixing under the definition and what does not, which will invariably lead to inconsistent decisions and thus inconsistent reporting.

For example, blockchains like Ethereum can be used to access an incredibly large and growing number of smart contracts that can be said to utilize “programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction,” which is a specific category of “protocol or service” that FinCEN identifies as involving CVC mixing under the current definition. Some of those smart contract protocols also allow for the pooling and exchanging of assets, which are two other illustrative examples of CVC mixing included by FinCEN in the proposed definition. The definition would, therefore, require financial institutions to determine whether virtually every single smart contract that a user may interact with facilitates CVC mixing.

One financial institution may conclude that a commonly used decentralized financial protocol that facilitates the pooling and exchange of assets constitutes CVC mixing under the definition. On the other hand, another financial institution may conclude that such a protocol does not involve CVC mixing because all transactions within the protocol are transparent and thus the source of funds can ultimately be traced using sophisticated blockchain analysis.

This type of discretionary decision will need to be made countless times over every conceivable form of decentralized finance protocol as well as with respect to every third party service, wallet service, cross-chain bridge, privacy protocol and any other service that facilitates CVC transactions in a manner other than the most traditional direct transfer from one wallet address to another. Not only will this process be incredibly burdensome, but FinCEN is likely to see inconsistent reporting across financial institutions based on unique

interpretations of the broad definitions in the proposal. FinCEN is also likely to receive reports on the same transaction from financial institutions but in a fragmentary way due to varying interpretations that FinCEN then must resolve internally to make sense of the reporting.

Identifying and labeling different types of service providers operating on the blockchain is at the core of our business at Chainalysis. From our experience, the key to generating reliable and useful data about on-chain activity is clear definitions based on tangible factors that can be implemented at scale. The current definition of CVC mixing in the proposal lacks the necessary clarity to serve as the foundation for an effective reporting regime and will hinder FinCEN's efforts to gain valuable data about CVC mixing.

- B. The broad definition of CVC mixer will likely result in excessive reporting on transactions with no association to illicit activity.

To the extent that there will be consistency in reporting, it will likely be in favor of over-reporting on transactions having no association with illicit activity. The definition of a CVC mixer in the proposal is incredibly broad and includes “any person, group, service, code, tool, or function” that “obfuscates the source, destination, or amount involved in one or more transactions.” This definition can be interpreted as applying to countless services that would otherwise not be considered mixers.

As alluded to above in the discussion about how Chainalysis labels mixers in our data, virtually every type of identifiable service has the impact of obfuscating the source, destination, or amount of a CVC transaction. This is due to the fact that when users send cryptocurrency to a service such as CVC exchanges, their assets do not just sit at the initial deposit address. Instead, the service moves the assets around internally as needed, pooling it with the funds of other users as needed or to meet regulatory requirements. For instance, many exchanges transfer portions of deposited funds in cold wallets disconnected from the internet for security reasons. Therefore, it does not make sense to attempt to trace a transaction through a service provider as it is no longer possible to determine which assets are associated with the original sender of a transaction. Under the proposed definition, this would mean that virtually every service provider would be considered a CVC mixer.

FinCEN proposes an exception to the definition of CVC mixing for such internal protocols or processes at certain types of financial institutions that “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.” As a result, under the proposal, a financial institution conceivably would not need to report to FinCEN

about a customer transaction traceable to another financial institution subject to AML requirements. However, in practice, this exception will be incredibly difficult to implement into a compliance process as not all wallet addresses are easily attributable to a specific service, and even when they are, it may not be clear whether that service is preserving the necessary records to take advantage of the exception. As a result, financial institutions will be left in the position of filing reports to FinCEN anytime a transaction is traceable to a third party service even when that service is not intended to serve as a CVC mixer and a user is interacting with the service for commercial purposes unrelated to illicit activity.⁷

Although FinCEN explains that the proposal is intended to comprehensively capture CVC mixing activity, the excessive reporting that will be created by the current broad definitions would likely prove to be disadvantageous to FinCEN. FinCEN may be inundated with irrelevant reporting and voluminous filings that serve only to clog an otherwise already overly crowded reporting system making it increasingly difficult to sift through and find the reporting of significance. This will also place an excessive burden on compliance staff at financial institutions and may lead to compliance failures and breakdowns in other areas. Finally, excessive reporting may implicate privacy concerns worth further analysis.

- C. There is no explanation in the proposal for how the foreign nexus requirement should be applied in the context of blockchain transactions.

Under Section 311 of the Patriot Act, FinCEN may only adopt special measures relating to transactions involving foreign jurisdictions. To that end, the proposal is limited in its applicability to transactions “within or involving a jurisdiction outside the United States.” However, this requirement that CVC mixing activity have a foreign nexus is not explained in the proposal and leaves open questions about what is required for a reportable transaction in the context of blockchain transactions.

It may be easy to conclude that the foreign nexus requirement is met when a financial institution services a customer based outside the United States or when a financial institution sends funds to a centralized CVC mixer known to be operating outside the United States. However, it seems clear that FinCEN also intends to capture mixing activity that occurs through on-chain protocols, wallet services, and other means that may not have a clearly defined association with an individual or company with a known location. Indeed,

⁷ By way of another example that could result in excessive and unnecessary reporting, FinCEN identifies the use of single-use addresses as an example of CVC mixing. However, many Bitcoin wallets are designed with software that generates new wallet addresses for every transaction. Indeed, data suggests that approximately 50% of all Bitcoin transactions are sent to previously unused addresses. See <https://blog.bitmex.com/bitcoin-address-re-use-statistics/>. Under the proposed definitions, every Bitcoin transaction from wallet providers who follow best practices would arguably be reportable.

when discussing the foreign nexus requirement, FinCEN uses the phrase “non-mixer CVC mixing,” which seemingly refers to mixing that does not occur through a traditional service that would have an identifiable location - for example, CVC mixing that occurs through an on-chain smart contract protocol cannot be associated with any single jurisdiction.

Despite the complexities presented by such examples, the proposal is silent on what factors financial institutions should look to in deciding whether a foreign nexus exists. It is unclear whether FinCEN expects financial institutions to simply assume no foreign nexus exists absent demonstrable evidence to the contrary or if financial institutions need to analyze particular elements of a transaction to make a determination on jurisdiction.

There are also practical limitations that FinCEN should consider when determining how to identify a foreign nexus. Specifically, even if a wallet address can be linked to an identifiable service such as a CVC mixer, it is significantly more difficult to attribute that address or service to a particular location. Absent a CVC mixer identifying their location, blockchain analysis and other tooling must generally leverage geolocation data of a website associated with the service.

- D. FinCEN should revise the definitions in the proposal to clearly delineate the type of CVC mixing activity that is subject to the special measures.

To address the issues set forth above, Chainalysis recommends that FinCEN narrow and clarify the scope of the definitions in the proposal to ensure consistent reporting that captures the type of activity that presents the highest risk of potential involvement with illicit finance.

As an initial matter, FinCEN should abandon the attempt to define CVC mixing in terms of broad categories of activity that may have the effect of obfuscating the source, destination, or amount of a CVC transaction. Instead, FinCEN should define CVC mixing to capture only those services that are designed with the purpose of providing users a means of obfuscating the source, destination, or amount of a transaction. This would result in reporting on transactions involving those platforms that are most often leveraged by bad actors without unnecessarily capturing otherwise legitimate transaction activity.

FinCEN should also narrow the definition of CVC mixers to individuals or groups of individuals who operate a mixing service. The current definition creates confusion by including technical concepts such as “code” or a “function” as a CVC mixer. A definition limited to identifiable individuals will make the reporting requirement more productive by

helping direct FinCEN to those service providers who may be compelled to assist in an investigation.

Finally, FinCEN should clarify which factors a financial institution must analyze to determine whether a foreign nexus exists. Further, financial institutions should only be required to report on transactions that they know or have reason to know involve a jurisdiction outside of the US so that liability is appropriately constrained considering the practical difficulties of identifying the location of certain services operating on blockchain networks.

II. There is an insufficient basis to conclude that the special measures will be effective in deterring bad actors from leveraging mixers for illicit activities.

Beyond the practical difficulties of implementing the proposed special measures, Chainalysis is also concerned that the special measures will not have the desired effect sought by FinCEN. The proposal states that the primary goals for implementing the special measures are to “discourage the use of CVC mixing by illicit actors” and “to better understand the illicit finance risk posed by CVC mixing and investigate those who seek to use CVC mixing for illicit ends.”

Customers of FinCEN-registered financial institutions know that those institutions gather “know your customer” (KYC) information on them, considering that they must provide such information upon becoming a customer. Moreover, it is generally understood that financial institutions must implement AML programs that typically involve transaction monitoring for suspicious activity. Therefore, to the extent that a bad actor utilizes a financial institution for CVC transactions, it is almost certain that those bad actors are already aware that the institution is monitoring their transactions for suspicious activity and have access to KYC information that it will report to FinCEN in the instance that there may be evidence of illicit activity.

The proposal seems to posit that there is a class of bad actors who have been using financial institutions to move assets to and from CVC mixers for illicit transactions but who are not sufficiently deterred by the existing AML regime in place. This seems highly unlikely, particularly with respect to state-sponsored actors, like the Lazarus Group and Russian ransomware operators, who seem to be the focus of the proposal. But even if the existing KYC and risk-based reporting regime is not already a deterrent, there is no stated rationale or evidence in the proposal as to why mandatory reporting of certain transactions will somehow change that calculus and discourage customers from using mixers for illicit purposes. It is simply assumed that the special measures will have this effect even though experience and logic would suggest otherwise.

In terms of FinCEN's second stated objective of obtaining a better understanding of the risks posed by CVC mixing, it is also unclear what mandatory reporting accomplishes that cannot already be obtained from publicly available information and the SAR reporting regime. The proposal does not explain what type of helpful information it expects to receive from the mandatory reporting regime that is not already captured. In fact, the opposite appears to be true when FinCEN states that it "believes that the existing risk-based approach to AML/CFT compliance used by covered financial institutions already largely encompasses the information FinCEN is requesting."

Ultimately, the primary challenge presented by CVC mixers is not due to a lack of information that can be remedied by mandatory recordkeeping and reporting. The transparent nature of the blockchain combined with well-calibrated risk-based reporting from financial institutions already provides a plethora of information by which to understand the use of CVC mixers by illicit actors. As a result, additional mandatory reporting will be less effective than alternative policy approaches, such as improved international cooperation and successful capacity building in jurisdictions where CVC mixers are operating to effectively mitigate the risks that FinCEN appropriately identifies in the NPRM.

III. A deeper investment in blockchain analysis solutions offers a more effective and less resource-intensive means for understanding and mitigating the illicit finance risks associated with mixers.

Although Chainalysis is concerned that proposed special measures may be ineffective in mitigating the risks presented by bad actors leveraging CVC mixers, we believe there are more effective and less resource-intensive means for developing a better understanding of these risks. Specifically, a deeper investment in blockchain analysis while leveraging existing SAR reporting would allow FinCEN and financial institutions to obtain a more granular view of transaction activity involving mixers and appropriately identify potential illicit activity in near-real time without reliance on overburdensome and ineffective additional reporting.

Using blockchain analysis, FinCEN and other relevant stakeholders can analyze all CVC flows into and out of identified mixers. Armed with that information, FinCEN would be able to trace individual transactions back to their source or to their ultimate destination to help understand if the funds have been involved in some sort of illicit activity. Moreover, with the specialized assistance of Chainalysis, FinCEN would even be able to leverage specialized assistance from Chainalysis to gain a more complete picture of the activity involved. All of this is possible without any reporting from financial institutions by leveraging the transparent nature of blockchains.

To the extent that potential illicit activity is observed by monitoring identified mixers, FinCEN would then be in a position to work with financial institutions to ensure that any activity linked to customers at those institutions is appropriately flagged and reported to FinCEN. Many financial institutions are already reporting SARs when customers interact with CVC mixers, which could supplement and validate the insights gained from monitoring mixing activity directly.

Leveraging blockchain analysis to monitor and trace mixing activity would be more effective than the current reporting regime contemplated under the proposed special measures. As currently constituted, the proposed rule would result in inconsistent and excessive reporting to FinCEN anytime a financial institution has a customer who transacts with CVC that is traceable to some sort of mixing activity, even if the mixing activity is done by a third party, occurred years in the past, or is completely unrelated to illicit activity. This type of reporting will not be helpful to FinCEN whereas a purpose-built monitoring system using blockchain analysis will.

—

Chainalysis thanks FinCEN for the opportunity to submit this comment and would be happy to provide more information behind our recommendations above if helpful.

For further inquiry, please contact:

Jason Somensatto
Head of North American Public Policy, Chainalysis
jason.somensatto@chainalysis.com