January 22, 2024

Via Electronic Submission

Financial Crimes Enforcement Network
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 - Docket Number FINCEN–2023–0016

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] is grateful for the opportunity to respond to the Financial Crimes Enforcement Network's ("FinCEN's") notice of proposed rulemaking (NPRM or proposed rule) requiring financial institutions ("FI(s)") to maintain certain recordkeeping and reporting requirements relating to transactions involving convertible virtual currency mixing.

ICBA appreciates FinCEN's approach to protecting the financial system from risks surrounding crypto mixing. However, we assert that FinCEN's proposed recordkeeping and reporting requirements for FIs are not enough to adequately protect American consumers and business entities from illicit financial activity that mixers pose. Designating crypto mixing as a "primary money laundering concern" is a first step, but it is not enough. It demands that the United States government recognize crypto mixing as a pressing national security threat, and it should be treated as such.

Background

"Convertible virtual currency" ("CVC") is a term to describe digital currency, cryptocurrency, stablecoins, and other digital assets that function as the equivalent or substitute for traditional currency. CVC operates on public blockchains that record every transaction. This history is visible to anyone with a web browser. By searching websites like Etherscan, anyone around the world can view these records and see every payment that has occurred.[2] While many within the cryptocurrency community see this as

[1] *The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation.*

As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at icba.org.

[2] "The Ethereum Blockchain Explorer," Etherscan, (2024), https://etherscan.io/.

an advantage over traditional systems, others have chosen to introduce enhanced measures and technologies to conceal key transactional details.

Various programs and companies like Tornado Cash and Blender.io developed anonymity tools like CVC mixing to dilute or eliminate transactional trails. As described within the proposal, CVC mixers can use different methods to obscure transactional trails, such as pooling multiple people's crypto assets together into a single wallet, thus concealing the identities of the parties or creating single-use accounts in a series of transactions that distort the destination of the transferred funds.

Unsurprisingly, these capabilities have turned crypto mixers into one of the most important elements in money laundering operations throughout the world. The proliferation of these capabilities has complicated law enforcement investigations and directly harmed the US economy and countless consumers. One of the most prolific users is North Korea, which frequently targets decentralized cryptocurrency exchanges and bridges to steal crypto assets. In the past six years, North Korean hackers have seized more than $3 billion worth of crypto assets[3] to fund "an unprecedented number of recent launches of ballistic missiles (including inter-continental ballistic missiles)."[4] This crypto-enabled illicit activity is a clear and present danger to the United States.

In recognition of North Korea's growing threat, the United States government has taken more steps to curb their use of crypto mixers. For example, in May 2022, the Office of Foreign Assets Control ("OFAC") sanctioned Blender.io, a virtual currency mixer operating on a Bitcoin blockchain, in response to the CVC mixing threats to cyber security. Additionally, the agency found that the DPRK used Blender.io to help launder more than $20 million stolen from Axie Infinity.[5] Likewise, OFAC discovered that Blender.io also facilitated money laundering for Russian-linked ransomware groups[6] and subsequently blocked the entity and users from conducting transactions.

In September 2022, OFAC went even further and sanctioned the well-known crypto mixer Tornado Cash for helping to launder more than **$7 billion** since its development in 2019.[7] More specifically, the agency cited Tornado Cash's key role in the largest cryptocurrency heist to date, the theft of $455 million in crypto assets from Axie Infinity. The DPRK-sponsored Lazarus Group used Tornado Cash to launder more than **$96 million**. In response to this illicit activity, the agency prohibited all U.S. citizens from transacting with Tornado Cash.

---

[3] CoinDesk, "North Korea Was Responsible for Over $600M in Crypto Thefts Last Year: TRM Labs," (January 5, 2024), https://www.coindesk.com/policy/2024/01/05/north-korea-was-responsible-for-over-600m-in-crypto-thefts-last-year-trm-labs/.

[4] The Financial Action Task Force, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," (2023), FATF, pg. 27, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf.

[5] The U.S. Department of the Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," (May 6, 2022), U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats | U.S. Department of the Treasury.

[6] Russian-linked ransomware groups such as Trickbot, Conti, Ryuk, Sodinokibi, and Gandcrab

[7] The U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," (August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

However, North Korean hackers and ransomware gangs are not the only users of crypto mixers. Increasingly, crypto mixers are utilized by bad actors who engage in "pig-butchering" scams, a growing type of fraud that involves criminals using social media to lure unsuspecting victims into a conversation by posing as an old friend, an investor, or a wrong number.[8] The scammers convince victims to invest in fraudulent virtual currency schemes, steal said currency or funds, and disappear. Pig-butchering scammers often use mixers to cover their tracks, thus complicating any efforts by the justice system to hold these criminals responsible.

The scale of pig-butchering scams is expanding at a staggering pace. In 2022, a Federal Bureau of Investigation report revealed that consumer losses from investment scams, a broad category that includes pig-butchering, climbed 127% over the previous year to a record $3.31 billion.[9] Unfortunately, this research likely undercounts the true toll on American consumers as it only captures the incidents that are *reported* to law enforcement.

In response to these ongoing threats of mixing-enabled criminal activity, FinCEN issued this NPRM and used its authority[10] to determine 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." With this conclusion, FinCEN now proposes that covered FIs should be subject to enhanced recordkeeping and reporting requirements to help the government investigate illicit activities. FinCEN states that these additional reporting obligations will only apply to covered financial institutions that directly engage in cryptocurrency transactions, and it should not apply to institutions with indirect exposure (e.g. a bank receiving funds from a cryptocurrency exchange associated with the sale of potentially mixed cryptocurrency).

Executive Summary

Over the past few years, North Korea has stolen billions of dollars' worth of crypto assets, laundered them with crypto mixers, and then funneled these ill-gotten gains directly into its weapons of mass destruction program. There are now more missiles sitting on North Korean launchpads and aimed at the United States and her allies as a direct result of the proliferation of crypto mixing capabilities. This threat is compounded by the fact that ransomware continues to plague the communities that our bankers serve. The message we have received from our bankers is loud and clear: The world is a more dangerous place today because cryptocurrency mixers exist, and the US government must act decisively to curtail this national security threat.

To that end, while ICBA recognizes the significance of FinCEN classifying crypto mixers as a "primary money laundering concern" and proposing enhanced recordkeeping and reporting requirements for financial institutions, we believe the severity of this threat to national security and the well-being of the

[8] The Financial Crimes Enforcement Network, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering,'" (September 8, 2023), pg.2, https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf.
[9] The Federal Bureau of Investigation, "2022 Internet Crime Report," pg. 12, 2022, IC3Report.pdf.
[10] 31 U.S.C. 5318A(a)(1)

US economy calls for a stronger approach targeted directly at the source of the problem: the cryptocurrency industry.

Ideally, we believe that the government should build on the work that OFAC started. However, we are still concerned because OFAC's actions have not stopped, nor can they compete with the rapid scale of technological development in the cryptocurrency ecosystem and their frequent attempts to circumvent US and global regulators. This threat demands a comprehensive approach across the government to curtail the use of crypto mixers, as well as address the related risks of the expanding DeFi ecosystem and the use of unhosted wallets.

While we appreciate FinCEN's approach to protecting the financial system from risks surrounding crypto mixing, we affirm that FinCEN's proposed preventative measures are not nearly enough to adequately protect American consumers and business entities from illicit financial activity that mixers pose and assert the following:

- This threat demands more action from the American government across the board to ensure that North Korean hackers, ransomware gangs, and pig-butchering criminal organizations can no longer hide their illicit activities from law enforcement agencies, national security organizations, prosecutors, and regulators.
- International collaboration is imperative.
- FinCEN should focus efforts on the entire crypto ecosystem; and
- Education is needed for community banks to fulfill the requirements of these new reporting rules.

ICBA's Comments

FinCEN Should Focus Its Efforts on Crypto Mixers and the Wider Crypto Ecosystem

The cryptocurrency ecosystem is composed of significant players and technologies that all have a hand in supporting illicit actors' ability to shroud their transactions with crypto mixers. One of the most important sectors is the burgeoning world of decentralized finance ("DeFi"), a term that broadly describes a shadow banking system of protocols on public blockchains that offer users products and services that mirror those of the traditional financial system. Among the most important parties in DeFi are decentralized exchanges and bridges, where users can quickly exchange one crypto asset for another or transfer to another blockchain in mere seconds. More often than not, cybercriminals will utilize DeFi exchanges and bridges to swap into different assets, including stablecoins, before using crypto mixers to complicate the investigative trail even more.

ICBA has long maintained that DeFi exchanges, along with every other entity in DeFi, should be held to the same standards as participants in the traditional financial system, including FinCEN recordkeeping and reporting requirements. FinCEN must work with other agencies and regulators to close the gaps presented by the current lack of regulation and enforcement in the DeFi ecosystem; otherwise, any effort aimed at curbing crypto mixing is bound to fall short.

Mixing technologies also do not spring forth from the internet independently—they are the products of deliberate choices by developers to give cryptocurrency users enhanced capabilities to hide critical information from regulators, law enforcement, national security organizations, and financial institutions. All too often, these developers seek ways to obfuscate legal or regulatory responsibilities by establishing so-called "decentralized autonomous organizations" or similar constructs. The creators of Tornado Cash tried such an approach; however, the Department of Justice alleges that Tornado Cash's decentralization was simply an illusion. In its indictment of Roman Storm and Roman Semenov, the government outlines how they retained and exerted control over the daily operations of Tornado Cash and played a key role in advertising its capabilities to prospective users.[11]

While we support the government's efforts to hold Tornado Cash's developers responsible for their actions, we believe that policymakers and regulators must take additional steps to adopt a "same activity, same risk, same regulatory treatment" approach towards DeFi entities. ICBA has consistently argued that "decentralization" in crypto is a fiction—every DeFi protocol, including mixers, is the result of decision-making by humans, coding by humans, governance by humans, and operations by humans.[12] These people, in turn, fulfill roles found in the regulated world of traditional finance, such as money transmitters or broker-dealers. Policymakers and regulators must be clear-eyed and craft a regulatory and enforcement regime that acknowledges these facts.

The reporting requirements will mandate that FIs directly involved with CVC mixing identify and report any mixing activity inside and outside the United States to FinCEN. The proposed rule will require FIs based in the United States to report within 30 calendar days of their initial detection of the transaction the amount and type of CVC used, the CVC wallet address associated with the mixer, the transaction hash, the date of the transaction; the IP addresses and timestamps; the email addresses of those associated with the mixer; the residential or business address of the customer engaged in a covered transaction; and the unique identifying number such as a Taxpayer Identification Number.[13]

The proposed rule would also require a narrative that describes the activity observed by the covered FI, the investigative steps taken, the information about the behavior, or other such details that the covered FI believes would aid investigations of the activity. FinCEN asserts that "as the covered financial institution would have insight into the normal pattern of its customers' transactions, this narrative would assist with understanding if there is an uncharacteristic change in pattern of behavior."[14]

---

[11] The United States Attorney's Office Southern District of New York, "Tornado Cash Founders Charged with Money Laundering and Sanctions Violations," (August 23, 2023), Southern District of New York | Tornado Cash Founders Charged With Money Laundering And Sanctions Violations | United States Department of Justice.
[12] Independent Community Bankers or America, "RE: Public Comment on IOSCO's Consultation Report on Policy Recommendations for Decentralized Finance (DeFi)" (October 18, 2023), https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/response-to-iosco-defi-policy-recommendations.
[13] Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 F.R. 72722 (proposed October 23, 2023) (to be codified at 31 C.F.R. 1010). Federal Register :: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern.
[14] 88 F.R. 72711.

ICBA agrees with FinCEN that such activity "presents an acute money laundering risk[15]" and merits a forceful response from the government. However, it is not enough to label it a "primary money laundering concern" and expect that additional reporting will deter criminals from using these technologies. The proposed rule will not be effective because FIs would be required to report mixing activity after it occurs. This begs the question: Is this enough to curtail criminal activity? None of the proposed rule requirements would have stopped or mitigated a situation like Tornado Cash. The crypto ecosystem allows for the instantaneous transfer of value around the world, and developers are constantly finding new ways to circumvent laws and regulations. For example, with unhosted wallets and decentralized protocols, criminals can easily exchange mixed cryptocurrencies with little, if any, knowledge from neither a regulated entity nor a government agency. We believe that significant gaps will remain unless FinCEN enhances its enforcement actions against all crypto entities that help to sustain the rising threat of crypto crime. The government must do much more to shield the US financial system and American consumers by prohibiting the use of crypto mixing technologies. Therefore, instead of introducing a new recordkeeping and reporting requirements for community banks, FinCEN should focus its efforts on confronting this problem at its source: the cryptocurrency industry. Our members vehemently contend that CVC mixing is too dangerous to be addressed in isolation and merely designated as a primary money laundering "concern." We strongly believe that FinCEN's reporting requirements will not adequately address the risks presented by the growing capabilities of the entire ecosystem.

Crypto Mixing Has No Legitimate Purpose

The NPRM notes that crypto mixing "may be used for legitimate purposes, such as privacy enhancement for those who live under repressive regimes," but there is little research to substantiate these claims. Instead, there are countless examples of criminals and malicious state-actors funneling billions through crypto mixers to cover their digital tracks. For instance, in 2021, the DOJ arrested Roman Sterlingov, the operator of Bitcoin Fog, for running the longest-mixing money laundering service since 2011.[16] Court documents indicated that Sterlingov moved over 1.2 million bitcoin, valued at **$335 million, for over a decade**. Likewise, the U.S. Attorney's Office for the Eastern District of Pennsylvania took down ChipMixer, one of the most widely used mixers to launder money, for stealing more than **$3 billion worth of cryptocurrency between 2017 and 2023**.[17] Bitcoin Fog's and Chipmixer's cases exemplify why CVC mixing, in its entirety, encourages destructive behaviors from illicit actors. Our members strongly contend that there are no legitimate uses for CVC mixing.

---

[15] 88 F.R. 72707.

[16] The U.S. Department of Justice Office of Public Affairs, "Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency Mixer," (April 28, 2023), https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

[17] The U.S. Attorney's Office Eastern District of Pennsylvania, "Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions," (March 15, 2023), https://www.justice.gov/usao-edpa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed.

International Collaboration

While motivations and methodologies for crypto-enabled criminal operations may differ, they all share one common trait: they frequently rely on crypto mixing to shroud their transactions from law enforcement and legal systems. The expansion of the crypto ecosystem presents criminals around the world with seemingly endless opportunities to attack US interests and launder assets. In recognition of this global activity, we urge FinCEN to take additional steps to work with international partners and strengthen enforcement actions against the crypto entities responsible for mixing**.**

Therefore, ICBA and its members also call on FinCEN to strengthen its collaboration with international partners to confront the threat of crypto mixing in unison. The speed and opacity offered by cryptocurrency transactions, combined with regulatory arbitrage afforded by lax regulatory schemes in other jurisdictions, calls for a multi-faceted approach with other countries to investigate criminal activity, bolster legal and regulatory frameworks, and ultimately hold criminals and any complicit crypto entities accountable for the harm they inflict. Likewise, if certain jurisdictions continue to serve as safe havens for crypto mixers and cybercriminals, then the US government should not hesitate to consider additional punitive measures.

FinCEN Should Clarify How Bankers Will Be Educated About Any New Requirements

Our members strongly urge FinCEN to specify how it intends to educate covered FIs on adequately identifying and separating mixing information that must be reported to FinCEN. According to FinCEN, covered FIs directly engaging in CVC mixing activity may use free or paid commercial software to detect mixing transactions while complying with current SAR and currency transaction report requirements. FinCEN notes that free direct and indirect programs can identify mixers if the program is "relatively stable and well known but could require supplementary manual investigative work to uncover**.**"[18] Free or paid commercial mixing software may be susceptible to hacker groups, like the Lazarus Group, that routinely operate in the crypto ecosystem. The NPRM does not specify if the government would dedicate representatives to educating FIs on CVC mixing identification.

Conclusion

OFAC has tried to limit the illicit activity by crypto mixers with the toughest sanctions the US government has to offer, but those actions were not enough to curb the danger. We urge FinCEN not to underestimate the threat presented by these technologies. Therefore, while we support FinCEN's approach to developing new ways to address the criminal activity involved associated with crypto mixing, we implore FinCEN to consider a wider range of actions to address the significant roles that DeFi protocols and unhosted wallets play in illicit finance. Actions against crypto mixers alone are not sufficient to curtail criminal activity stemming from the crypto world. We are confident a comprehensive approach would decrease the number of illicit actors, reduce national security risks,

[18] 88 F.R. 72717.

shield more consumers from crypto-related crimes, and provide greater security for community banks and the US financial system.

ICBA appreciates the opportunity to provide comments in response to this request. If you have any questions, please do not hesitate to contact me at Brian.Laverdure@icba.org or (202) 821-4427.

Sincerely,

/s/

Brian Laverdure, AAP
Senior Vice President, Digital Assets and Innovation Policy