Bitcoin Today Coalition

January 22, 2024

Financial Crimes Enforcement Network (“FinCEN”)
Department of the Treasury
Ms. Andrea Gacki, Director
PO Box 39
Vienna VA 22183

Response to FinCEN’s Request for Comment on Notice of Proposed Rulemaking (“NPRM”) Regarding Convertible Virtual Currency (“CVC”) Mixing, Docket Number FINCEN–2023–0016

Dear Director Gacki,

We appreciate the opportunity to comment on FinCEN's NPRM proposal to designate transactions involving CVC mixing as a class of transactions of primary money laundering concern. The Bitcoin Today Coalition (“BTC”) is a 501(c)(4) not-for-profit, non-partisan organization that advocates on behalf of American individuals’ and businesses’ rights to own, secure, and use their bitcoin. To do so, BTC focuses on leading educational efforts for policymakers, regulators, and others at the federal and state levels.

We support the adoption of bitcoin and its beneficial impacts on innovation. Consumers, investors, and businesses; global financial stability; technological and economic advances; safe and affordable financial services; national security; and future job growth all benefit from bitcoin. Its sound monetary properties promote financial inclusion and uplift those left behind by the traditional financial system. Our members represent a broad constituency; we work alongside entrepreneurs and innovators, veterans and national security practitioners, economic development professionals, and academia. Energy industry stakeholders and human rights activists endorse our cause as well.

Preventing financial crime is a goal that we share with FinCEN. The people we advocate for, everyday American individuals and businesses, are best served when criminals are prevented from using the financial system to funnel funds, whether it is dollars or bitcoin, to further their means. This does not mean that we believe the government should be permitted to censure, restrict, or ban technologies because criminals may abuse them. Nor do we believe the government should require third-party financial institutions to collect and send vast amounts of sensitive personal information to a centralized government database without a robust analysis of the impact on US citizens' fundamental rights to privacy and unreasonable search and seizure. As such, we respectfully disagree with FinCEN's proposed rule.

The proposed rule is overly broad

The proposed rule defines CVC mixing too broadly, encompassing a wide range of activities without demonstrating a clear link to illegal activity. This overreach captures legitimate uses of mixers, such as enhancing user privacy or obfuscating transaction pathways for security reasons. Such legitimate uses will be inadvertently chilled by the proposed rule's stringent reporting requirements, hindering technological innovation and advances in security practices. Bad actors already use information from public blockchain data to feed their phishing and social engineering schemes,[1] and defining common-sense privacy and security practices as a primary money-laundering concern puts consumers and businesses at risk. Indeed, a similar rule applied to data processing would effectively ban virtual private networks ("VPNs") and similar technologies, which are today widely accepted as ways to protect and enhance privacy and security for consumers and businesses.

The proposed definition of mixers not only includes technologies that may be used in transactions to enhance privacy, but also includes myriad other technologies that are not purpose-built for money laundering.[2] Some of these technologies strive to scale payment systems that would seek to compete with entrenched businesses, to enable local community financial services, and to promote self-custody of assets to reduce reliance on risky or unreliable counterparties.

[1] "How Cyber Criminals Target Cryptocurrency," Proofpoint, June 9, 2022. https://www.proofpoint.com/us/blog/threat-insight/how-cyber-criminals-target-cryptocurrency
[2] See the Bitcoin Policy Institute's letter in response to this NPRM at https://www.regulations.gov/comment/FINCEN-2023-0016-1611.

Imagine if FinCEN were concerned about criminals using techniques to layer proceeds from illicit activity in omnibus US dollar-denominated accounts at a financial institution. Compared to CVC transactions,[3] it is an undisputed fact[4] that the vast majority of money laundering and terrorism financing uses the US dollar and US dollar-denominated accounts at financial institutions,[5] especially the largest institutions[6] that are subject to FinCEN's jurisdiction.[7] If FinCEN took a similar approach to defining that transaction type as it does with defining CVC mixing, it would cripple the financial system with reporting requirements. It would also unintentionally sweep up the vast majority of legitimate transactions in an unconstitutional dragnet, requiring mountains of sensitive personal information be reported to and maintained by the government. This highly-sensitive, private information would be subject to attacks and compromises that have been repeated over and over in both the public[8] [9] and private[10] sectors.

The proposed rule lacks sufficient justification

The NPRM provides insufficient data and analysis to support the assertion that CVC mixing presents a significantly heightened money laundering risk, particularly compared to other financial transactions. Without a sound basis for such a sweeping designation, the rule is likely arbitrary and capricious. Despite FinCEN's access to millions of suspicious activity reports

---

[3] Jennifer J. Schulp et al., "Overstating Crypto Crime Won't Lead to Sound Policy," Cato Institute, January 27, 2023.
https://www.cato.org/blog/overstating-crypto-crime-wont-lead-sound-policy
[4] Department of the Treasury, "National Money Laundering Risk Assessment," 2022, https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf, p. 41.
[5] Carrick Mollenkamp, "HSBC became bank to drug cartels, pays for big lapses,' Reuters, December 11, 2012.
https://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211/
[6] Jonathan Stempel, "U.S. Judge accepts Danske Bank guilty plea in $2 bln pact to end Estonia probe," Reuters, January 5, 2023.
https://www.reuters.com/legal/us-judge-accepts-danske-bank-guilty-plea-2-bln-pact-end-estonia-probe-2023-01-05/
[7] Department of Justice, Southern District of New York, "Manhattan U.S. Attorney And FBI Assistant Director-In-Charge Announce Filing Of Criminal Charges Against And Deferred Prosecution Agreement With JPMorgan Chase Bank, N.A., In Connection With Bernard L. Madoff's Multi-Billion Dollar Ponzi Scheme," January 7, 2014.
https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-filing-criminal
[8] Jason Leopold et al., "The FinCEN Files," BuzzFeed News, September 20, 2020.
https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks
[9] U.S. House of Representatives, 114th Congress, Committee on Oversight and Government Reform, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," September 7, 2016.
https://oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/
[10] Tara Siegel Bernard et al., "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," New York Times, September 7, 2017.
https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

("SARs") that financial institutions file each year, the analysis and justification for this rule is noticeably lacking in analysis of such data. In a single instance in the background section for the rulemaking, FinCEN references its 2021 Report on Ransomware Trends in Bank Secrecy Act Data ("2021 Report")[11] that analyzed SARs from the brief period of six months from January to June 2021. The report identified 458 SARs containing suspicious transactions related to ransomware attacks that totaled $398 million. For reference, FinCEN discloses that it received 3,069,450 SARs in 2021,[12] meaning the number of SARs reviewed in the 2021 Report represented approximately 0.01 percent of SARs submitted in 2021.

Importantly, a SAR is not proof of criminal activity. SAR filings are often the result of alerts triggered by third-party surveillance systems, which have become commonplace in the financial services industry. Many of these third-party vendor solutions and associated regulatory technologies are riddled with inaccurate and false-positive results.[13] In fact, financial institutions face significant incentives to overreport activity through SARs since they face significant regulatory repercussions if they fail to report a SAR but face no repercussions for reporting activity that is useless.[14] Furthermore, many blockchain analytics solutions operate proverbial "black box" models that rely on behavioral clustering heuristics and loosely defined assumptions about transaction patterns to attribute pseudonymous blockchain activity to real-world entities; these solutions do not provide disclosures regarding their attribution methods and effectiveness.[15]

The NPRM suggests that the 2021 Report's SAR analysis identified $35.2 million in CVC value, or seemingly 8.8 percent of the total value linked to ransomware attacks, was subsequently routed through mixers. Unfortunately, FinCEN's analysis is flawed and relies on data that is inconsistent with the actual dates of activity identified in the report. The $35.2 million in value

---

[11] Department of the Treasury, Financial Crimes Enforcement Network, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," October 15, 2021. https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data

[12] Obtained from reports available at https://www.fincen.gov/reports/sar-stats. An important note is this figure may not represent all SARs received including those that were amended reports or reports regarding continuing activity.

[13] "The Truth About Suspicious Activity Reports," Bank Policy Institute, September 22, 2020. https://bpi.com/the-truth-about-suspicious-activity-reports/

[14] *Ibid*.

[15] Lily Hay Newman and Andy Greenberg, "Bitcoin Fog Case Could Put Cryptocurrency Tracing on Trial," Wired, August 2, 2022. https://www.wired.com/story/bitcoin-fog-roman-sterlingov-blockchain-analysis/

that was sent to CVC mixers is referenced in a table in Appendix 1 of the 2021 Report. That figure is an aggregation of all amounts tied to ten ransomware variants over a period of several years, sometimes dating as far back as July 2018. In FinCEN's own analysis of those variants, the total amount tied to the variants is $5.2 billion, of which *amounts sent to mixers represents less than one percent*. Indeed, the largest recipient of ransomware funds tied to the ten variants are CVC exchanges, totaling $2.6 billion or approximately half of the total. The other half of the total amount, $2.3 billion, is labeled "other" and includes "unidentified CVC services as well as unspent and untraced CVC."[16] There is no analysis of whether the predicate crime was reported to or already identified by law enforcement, whether the bad actors were identified and held to account despite the absence of the proposed rule, or whether the amount of funding sent to mixers relative to other prevalent transaction behaviors in financial crime is significant enough to warrant such a rule.

Unfortunately, the underlying data that FinCEN relies on to support the proposed rule is not available for public review and analysis. FinCEN does not publish comprehensive SAR data, even in a sanitized and aggregated form, on any regular basis. Indeed, Congress has called upon FinCEN[17] repeatedly[18] to release more data regarding the intelligence it collects so that the parties subject to its rules may learn from and strengthen their own programs. We strongly urge FinCEN to conduct a robust analysis of the data and to make sufficient data available to the public to bolster confidence in FinCEN's justifications for its existing and proposed rules.

The proposed rule is incompatible with risk-based AML approaches

FinCEN's existing regulations require financial institutions to develop and implement effective, risk-based anti-money laundering ("AML") programs. These programs should use customer due diligence and transaction monitoring practices tailored to the specific risks presented by each customer and their financial activities. By imposing blanket reporting requirements for all CVC mixing transactions, regardless of individual risk factors, the proposed rule undermines the effectiveness of risk-based AML programs. It hinders financial institutions from tailoring their

[16] "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," October 15, 2021, p. 16.
[17] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56 115 Stat. 308 (2001). https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[18] Anti-Money Laundering Act of 2020, Pub. L. No. 116-283 134 Stat. 4571-4572 (2021). https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf

AML compliance efforts to address the unique threats they face, potentially leading to inefficient resource allocation and reduced detection of actual suspicious activity.

Since 2003, FinCEN has emphasized the importance of a risk-based approach to combating illicit threats. For the last 20 years, this message has been repeated across dozens of joint statements,[19] fact sheets,[20] formal guidance,[21] and rulemakings.[22] In June 2021, FinCEN reinforced its longstanding position with a congressionally-required national list of anti-money laundering priorities ("National Priorities").[23] This publication was a welcome shift away from technical compliance and onerous form reporting to a more effective threats-based and outcomes-oriented approach to combating financial crime.

Further to that point, threats are not uniform across the CVC industry. Illicit actors each exploit, launder, and use CVCs differently. While hacks and exploits may occur in one corner of the ecosystem, the profits may be realized in another. Real-world observations suggest that the tactics, techniques, and procedures used by illicit actors vary widely[24] across the cryptocurrency ecosystem. North Korean and Russian cybercriminals continue to exploit obscure Proof-of-Stake ("PoS") tokens,[25] unsecure Decentralized Finance ("DeFi") Protocols,[26] fragile

---

[19] Board of Governors of the Federal Reserve System et al., "Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence," July 6, 2022. https://fincen.gov/news/news-releases/joint-statement-risk-based-approach-assessing-customer-relationships-and

[20] Department of the Treasury, Financial Crimes Enforcement Network, "Bank Secrecy Act Effectiveness and Efficiency Fact Sheet," June 2007. https://fincen.gov/sites/default/files/shared/bsa_fact_sheet.pdf

[21] Department of the Treasury, Financial Crimes Enforcement Network, "Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions," August 3, 2020. https://fincen.gov/sites/default/files/2020-08/FinCEN%20Guidance%20CDD%20508%20FINAL_2.pdf

[22] Department of the Treasury, Financial Crimes Enforcement Network, "Customer Due Diligence Requirements for Financial Institutions," 81 FR 29398, May 11, 2016. https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions

[23] Department of the Treasury, Financial Crimes Enforcement Network, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," June 30, 2021. https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

[24] "Illicit Crypto Ecosystem Report," TRM Labs, June 2023. https://www.trmlabs.com/report

[25] Erin Plante, "$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit," Chainalysis, September 8, 2022. https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/

[26] "DeFi, Cross-Chain Bridge Attacks Drive Record Haul from Cryptocurrency Hacks and Exploits," TRM Labs, December 16, 2022.

smart contracts, and vulnerable PoS cross-chain bridges[27] to steal billions of dollars annually. They then use a combination of DeFi chain hops,[28] Ethereum-based mixers,[29] and offshore exchanges[30] to obfuscate and ultimately cash out their illicit proceeds. Illicit gains from cyberattacks, cybercrimes, fraud,[31] and corruption are cashed out for local currency, but are increasingly cashed out in stablecoins.[32]

For domestic financial institutions, risk is highly dependent on the types of CVCs businesses they choose to support, the way they deliver their services, and jurisdictions they support. Indeed, no two businesses are the same. To combat illicit finance and support FinCEN's priorities, every domestic financial institution must prioritize its resources to address the most applicable threats to its business. Through the uniform categorization of an entire class of transactions as a primary money laundering concern, the proposed rule unnecessarily restricts domestic financial institutions' ability to align their BSA/AML programs against the real-world threats they face.

The proposed rule is duplicative

The proposed rule's mandatory reporting requirements largely duplicate existing requirements for suspicious activity reporting. FinCEN's existing AML framework already requires financial institutions to report suspicious transactions involving CVC mixing, including those that raise concerns about potential money laundering or other illicit activity. Indeed, rather than creating

---

https://www.trmlabs.com/post/defi-cross-chain-bridge-attacks-drive-record-haul-from-cryptocurrency-hacks-and-exploits

[27] "Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk," Chainalysis, August 2, 2022. https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/

[28] "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," Chainalysis, January 13, 2022. https://www.chainalysis.com/blog/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/

[29] "U.S. Treasury Sanctions Widely Used Crypto Mixer Tornado Cash," TRM Labs, August 8, 2022. https://www.trmlabs.com/post/u-s-treasury-sanctions-widely-used-crypto-mixer-tornado-cash

[30] "Behind Suex.io: the first sanctioned cryptocurrency exchange," TRM Labs, September 21, 2021. https://www.trmlabs.com/post/behind-suex-io-the-first-sanctioned-cryptocurrency-exchange

[31] Department of Justice, Office of Public Affairs, "Four Individuals Charged for Laundering Millions from Cryptocurrency Investment Scams," December 14, 2023. https://www.justice.gov/opa/pr/four-individuals-charged-laundering-millions-cryptocurrency-investment-scams

[32] Department of Justice, Office of Public Affairs, "North Korean Foreign Trade Bank Representative Charged in Crypto Laundering Conspiracies," April 24, 2023. https://www.justice.gov/opa/pr/north-korean-foreign-trade-bank-representative-charged-crypto-laundering-conspiracies

additional and costly reporting burdens for businesses in the US, we suggest it is more effective to focus on improving the suspicious activity reporting regime and highlighting the predicate crimes of illicit activities through FinCEN's National Priorities.

We highlight that the redundant reporting burden imposed by the proposed rule adds unnecessary complexity and compliance costs without adding significantly to FinCEN's existing intelligence-gathering capabilities. Many of the businesses that we advocate for have expressed grave concern about the excessive burden and costly reporting requirements under the proposed rule. Furthermore, it does not accomplish the underlying objective of the suspicious activity reporting requirement, which is to aid law enforcement in its duty to hold bad actors accountable. Much of FinCEN's existing intelligence data, in the form of SARs, goes unused by law enforcement agencies, whether due to the limited value of SAR data or due to limited resources at law enforcement agencies.[33] Therefore, it is premature to add to existing data through a burdensome and potentially duplicative reporting requirement that would include reporting highly sensitive personal data, without first assessing the effectiveness of existing data. Law enforcement agencies already use the same tools referenced in this NPRM to successfully identify and pursue criminal activity, and requiring financial institutions to adopt an additional layer of reporting will not enhance law enforcement's existing capabilities.[34]

A more sensible approach to combating illicit activity

We are aligned with FinCEN's goal to fight financial crime. The vast majority of US citizens and businesses that choose to use bitcoin and CVCs are not criminals, just as the vast majority of US citizens and businesses that choose to use the US dollar are not criminals. Simply declaring a privacy and security-enhancing technology as unsavory because criminals may use it is not a sound policy. If that were the case, VPNs, cryptography, multi-factor authentication, complex passwords, and many other technologies should be deemed inappropriate as well.

Instead, we urge FinCEN to focus on ensuring that financial institutions adopt effective, risk-based AML programs. We implore you to use the tools already at your disposal, such as the SAR regime, to enable law enforcement to effectively hold bad actors accountable. We ask you

[33] "The Truth About Suspicious Activity Reports," Bank Policy Institute, September 22, 2020.
[34] Andy Greenberg, "Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site," Wired, April 7, 2022.
https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

to analyze the data available to you to adopt national priorities that will help businesses steer their limited resources to the most critical financial crimes risks that the US faces.

Conclusion

FinCEN should reconsider its proposed rule on CVC mixing or withdraw it entirely. Existing AML regulations, when applied effectively through risk-based approaches, are sufficient to address the potential money laundering risks associated with CVC mixing without unnecessary burdens on legitimate users and financial institutions. We encourage FinCEN to focus its efforts on providing clear guidance to financial institutions, publishing comprehensive financial crime data and threat analysis, and supporting the development of robust AML programs tailored to the specific characteristics and risks of CVC transactions. We also suggest FinCEN conduct further research and analysis to establish the scope and preponderance of CVC mixing as a method for obfuscating illicit financial activity versus other methods that are renowned for their use in organized crime and state-sponsored terrorism. We urge FinCEN to focus and improve its existing tools, such as the SAR regime, to effectively empower law enforcement to hold bad actors to account without compromising the privacy and security of individuals and businesses.

Thank you for your time and consideration. We are always available for discussions on this topic or any related topics regarding bitcoin; please contact us at info@bitcointodaycoalition.org. We look forward to engaging in further dialogue on this important issue.

Sincerely,

CJ Wilson, Chairman
Alexander Brammer
Jayson Browder
Alexandra DaCosta
Robert Malka
Joshua Preston
Donna Redel

Bitcoin Today Coalition Board of Directors