



January 22, 2024

United States Department of the Treasury  
Financial Crimes Enforcement Network  
P.O. Box 39  
Vienna, Virginia 22183

Submitted electronically via regulations.gov

**Re: Ensuring Responsible Development of Digital Assets; Request for Comment**

Coinbase Global, Inc. (Coinbase) submits this written comment in response to the Financial Crimes Enforcement Network’s (FinCEN) notice of proposed rulemaking (NPRM) that proposes requiring domestic financial institutions to implement recordkeeping and reporting requirements on transactions involving convertible virtual currency (CVC) mixing.<sup>1</sup> This NPRM comes at a time of enormous opportunity for the United States to lead the world in digital asset innovation, but this opportunity depends in significant part on U.S. regulators, like FinCEN, creating a regulatory landscape that fosters the growth of compliant companies while holding accountable those that fail to meet their obligations.

As a leader in the CVC ecosystem, Coinbase fully supports effective regulation developed with the input and coordination of industry members. But we do not believe this proposed NPRM is an effective regulation for two key reasons:

*First*, FinCEN has not identified a *regulatory gap* that the NPRM would fill. Regulated virtual asset service providers (VASPs) are already subject to comprehensive recordkeeping and reporting rules that require them to file Suspicious Activity Reports (SARs) on illicit CVC mixing activity. Both the FATF and European Banking Authority (EBA) have recommended that financial institutions address any risks posed by CVC mixing through these *existing* SAR reporting procedures. The NPRM fails to explain why these existing requirements are inadequate to FinCEN’s purposes.

*Second*, with no regulatory gap to fill, the NPRM will lead to bulk reporting of data of little help to law enforcement. As the NPRM acknowledges, some CVC mixing is “used for legitimate purposes.”<sup>2</sup> Nonetheless, the NPRM includes an expansive definition of “CVC mixing” activity and does not include any monetary threshold for recordkeeping or reporting obligations. This is

---

<sup>1</sup> See Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, RIN 1506-AB64 (proposed Oct. 23, 2023) (hereinafter the “NPRM”).

<sup>2</sup> NPRM at 21 (referencing privacy only a few times in an 80 page document).

not simply a misuse of VASPs' finite compliance resources; it is *exactly* the kind of bulk reporting that Congress has explicitly discouraged.

In light of these critical problems, Coinbase believes that the NPRM should not be made a final rule. But, if FinCEN nonetheless decides to finalize a rule on CVC mixing, we recommend that it make the following changes to the current proposal:

*First*, instead of imposing new requirements, FinCEN should help VASPs be more effective in performing their existing obligation to file SARs on suspicious activity involving CVC mixing. For example, FinCEN could issue advisories, alerts, and guidance on CVC mixing trends, typologies, and indicators, along with expanded keyword searching (as FinCEN has done in many other areas).

*Second*, if FinCEN insists on new requirements outside of SARs, it should at least establish a monetary threshold to avoid triggering reporting of an enormous volume of low-value transactions. Indeed, FinCEN's other bulk reporting requirements (e.g., CTRs and CMIRs) are limited to transactions over \$10,000, and a similar approach is justified here. Such a threshold would prevent the unhelpful reporting of bulk amounts of legitimate transactions and preserve VASPs' finite compliance resources for other, higher impact efforts.

*Third*, even when the threshold is met, the NPRM should at most require recordkeeping—not reporting—to avoid the significant privacy and security risks inherent in a new centralized FinCEN repository of highly sensitive information. This change is particularly critical if the NPRM proceeds with a low or no threshold at all, since the burden and risks of such a repository increase with the volume of reported transactions. A recordkeeping requirement would fully serve the NPRM's stated purpose of ensuring that law enforcement can quickly obtain this information when needed.

*Finally*, regardless of the approach taken, FinCEN should provide a roadmap for how it and industry will technically implement the rule and a reasonable period of time to do so. Including a "sunrise" period would be consistent with FinCEN's prior rulemakings involving bulk data collections, and would provide a more practical opportunity for industry to come into effective compliance.

The NPRM's current failure to consider these less restrictive regulatory alternatives is inconsistent with the Administrative Procedures Act and other federal policy directives on privacy, security, and bank de-risking. Indeed, the NPRM's expansive targeting of privacy enhancing technology is at odds with FinCEN's own policy directives around technology and privacy, and inconsistent with its fundamental mission of protecting the American people and our financial system.

**I. CVC Mixing is an important privacy and security tool with many legitimate purposes, while illicit uses are the exception and would not even be captured by the NPRM.<sup>3</sup>**

While the NPRM acknowledges that CVC mixing “may be used for legitimate purposes,” it only superficially addresses the benefits of those legitimate purposes.<sup>4</sup> CVC mixing allows consumers to protect themselves while transacting on public blockchains—in which a single connection between an individual and a blockchain address can disclose that individual’s complete financial history.<sup>5</sup> There is nothing suspicious or illicit in desiring such a modicum of financial privacy from the world. Indeed, blockchain analytics show that the majority of CVC sent to mixing services in 2022 came from legitimate sources,<sup>6</sup> and more generally, money laundering accounted for only one half of one percent of all cryptocurrency transaction volume in 2021.<sup>7</sup> Accordingly, the majority of CVC mixing activity has enhanced the privacy and security of legitimate cryptocurrency transactions.<sup>8</sup> As detailed below (see Section IV), FinCEN should account for these privacy and security benefits before making the NPRM a final rule.

---

<sup>3</sup> This section responds to the NPRM’s general request for input, as well as the following question: “1. Does FinCEN accurately account for the burden and impact of this proposed rule when a covered financial institution knows, suspects, or has reason to suspect a transaction involves CVC mixing?”

<sup>4</sup> NPRM at 21 (referencing privacy only a few times in an 80 page document).

<sup>5</sup> See, e.g., Jan Henrik Ziegeldorf et al., *Secure and Anonymous Decentralized Bitcoin Mixing*, 80 *Future Generation Computer Systems* 448-466 (2018) (noting that CVC mixing is a useful tool to protect consumer financial privacy on the bitcoin blockchain because a consumer’s bitcoin wallet address can be linked to his IP address, enabling a third-party to identify the consumer’s complete financial history on the bitcoin blockchain).

<sup>6</sup> See Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over \$1 Billion in Illicit Funds in 2022*, <https://www.chainalysis.com/blog/crypto-money-laundering-2022/> (last visited Nov. 30, 2023) (finding that 76% of CVC sent to mixers in 2022 came from legitimate sources).

<sup>7</sup> See Chainalysis, *DeFi Takes on Bigger Role in Money Laundering but Small Group of Centralized Services Still Dominate*, <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/> (last visited Nov. 30, 2023).

<sup>8</sup> See Plaintiffs’ Motion for Partial Summary Judgment at 8, *Van Loon et al. v. Dep’t of the Treasury et al.*, No. 1:23-cv-00312-RP (W.D. Tex. Sept. 8, 2022) (discussing the following examples of legitimate uses of CVC mixing: (i) consumers have donated funds to the Ukrainian government’s publicly posted cryptocurrency wallet address via mixers following Russia’s invasion—donating to the Ukrainian government from a wallet address not linked to a consumer’s identity (i.e., post-mixing) reduces the risk that malicious actors affiliated with Russia would link the donation to the consumer and retaliate against the consumer; and (ii) consumers have recognized the effectiveness of using a CVC mixer when running a blockchain node from their homes to mitigate the risk of physical or virtual attacks associated with running a blockchain node).

By contrast, non-compliant offshore VASPs pose a far greater and ongoing illicit finance threat than CVC mixing. The U.S. Treasury and the Department of Justice (DOJ) have highlighted this threat.<sup>9</sup> While a growing number of countries impose compliance obligations on VASPs, there are still large gaps in global enforcement efforts.<sup>10</sup> A number of VASPs take advantage of these gaps by engaging in jurisdictional arbitrage—providing crypto services to global customers while having weak (or non-existent) AML controls, with the expectation that regulators will not hold them accountable.<sup>11</sup>

The evidence demonstrates that illicit actors—ransomware groups, sanctioned entities, darknet markets, scammers, and other cybercriminals—have sought out non-compliant VASPs to monetize their crimes.<sup>12</sup> This is no mystery, as criminals prefer VASPs they know require minimal (if any) KYC information, will not restrict their customers from exchanging funds with illicit counterparties, and will not file SARs with government authorities. Moreover, because non-compliant offshore VASPs receive the majority of illicit crypto transactions, it also makes sense they would receive the majority of illicit CVC mixing transactions.<sup>13</sup> This would include

---

<sup>9</sup> See U.S. Dep’t of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* 5 (Sep. 20, 2022), <https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf> (noting that “[t]he most significant illicit financing risk associated with virtual assets stems from VASPs operating abroad with substantially deficient AML/CFT programs . . .”); Dep’t of Justice, *The Role of Law Enforcement in Detecting Investigating, and Prosecuting Criminal Activity Related to Digital Assets* 7 (Sep. 6, 2022) (noting that “many digital asset exchanges and platforms make little or no effort to comply with anti-money laundering regulations . . . or operate in jurisdictions without anti-money laundering and countering-the-financing-of-terrorism (AML/CFT) requirements in line with the international standards”).

<sup>10</sup> U.S. Dep’t of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* 5 (Sep. 20, 2022), <https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf> (noting that “VASPs may choose to operate in jurisdictions with minimal or nonexistent AML/CFT requirements, weak supervision of their legal frameworks, or both.”)

<sup>11</sup> See *id.* (noting that “[u]neven and often inadequate regulation and supervision internationally allow illicit actors to engage in regulatory arbitrage, which is particularly concerning given the near-instantaneous and border-less nature of virtual asset transfers.”).

<sup>12</sup> See Chainalysis, *The 2021 Crypto Crime Report*, 9, 13, 74 (Feb. 16, 2021), <https://go.chainalysis.com/2021-Crypto-Crime-Report.html> (highlighting that “[cybercriminals] rely on a surprisingly small group of service providers to liquidate their crypto assets,” including “money services businesses with lax compliance programs”); Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders* 10 (2020), [https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20\(All%20Assets\)/Typologies\\_Concise%20Guide\\_12-20.pdf](https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf) (“Criminals deliberately seek out exchanges they know they can exploit with little or no obstruction when moving between fiat and cryptoasset, or from cryptoasset-to-cryptoasset.”).

<sup>13</sup> See, e.g., Chainalysis, *The 2023 Crypto Crime Report*, 5 (Feb. 2023), [https://go.chainalysis.com/rs/503-FAP-074/images/Crypto\\_Crime\\_Report\\_2023.pdf](https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf) (noting that Russia-based crypto exchange “Garantex . . . accounted for the majority of sanctions-related transaction volume [in 2022].”); U.S. Dep’t of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 29 (Apr. 2023) (noting that in 2022 “the most significant illicit financing risk associated with virtual assets stemmed from VASPs operating abroad with substantially deficient AML/CFT programs, particularly in jurisdictions where AML/CFT standards for virtual assets are nonexistent or not effectively implemented.”).

custodial mixer services that operate offshore to evade the BSA.<sup>14</sup> Because these offshore VASPs and custodial mixer services are unlikely to comply with the NPRM, the new reporting rules will yield little information about *illicit* CVC mixing. Rather, reports will come predominantly from compliant domestic VASPs with primarily *legitimate* CVC mixing activity to disclose—which does not serve the NPRM’s stated goal of increasing law enforcement transparency into illicit CVC mixing activity.

## **II. Rather than close any gap, new record-keeping and reporting requirements will only move resources away from more valuable compliance work.<sup>15</sup>**

### **A. Regulated domestic VASPs are already required to conduct KYC and file SARs on suspicious activity, including CVC mixing, which FinCEN can make more effective by issuing alerts or guidance to industry coupled with added keyword searching (as it has done in many other areas).**

Regulated U.S. VASPs are already obligated to carry out traditional compliance measures—such as filing SARs, risk rating customer transactions, and carrying out additional due diligence on customers when warranted—on all types of transactions, including CVC mixing (defined in the NPRM as “the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions”).<sup>16</sup> If a customer engages in *suspicious* activity related to CVC mixing over a \$2,000 threshold, the current SAR filing obligation already applies, and this reporting rule covers any transaction “designed to evade the requirements of the [BSA], whether through structuring or other means.”<sup>17</sup>

---

<sup>14</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2019-G001, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (2019) (establishing that the BSA covers custodial mixing activity because a custodial mixer is an “anonymizing service provider” and “an anonymizing services provider is a money transmitter under FinCEN regulations.”); see also FinCEN, U.S. Dep’t of the Treasury, FIN-2012-A001, Foreign-Located Money Services Businesses (2012) (establishing that foreign-located money services businesses servicing customers located in the U.S. are financial institutions under the BSA and therefore must comply with the relevant recordkeeping, reporting, and AML program requirements under the BSA).

<sup>15</sup> This section responds to the NPRM’s general request for input, as well as the following questions: “1. Does FinCEN accurately account for the burden and impact of this proposed rule when a covered financial institution knows, suspects, or has reason to suspect a transaction involves CVC mixing?”; “2. Is there a less burdensome way of collecting information regarding the details of a CVC transaction, which the BSA’s AML/CFT objectives require financial institutions to collect, including know-your-customer and customer due diligence?”; “8. What impact will this proposal have on augmenting law enforcement’s ability to track and trace CVC derived from cyber heists, ransomware, or similar illicit activity to aid the return of victim’s CVC?”.

<sup>16</sup> NPRM at 75.

<sup>17</sup> As regulated financial institutions under the Bank Secrecy Act, VASPs must file a suspicious activity report for any transaction (or a pattern of transactions of which the transaction is part) that involves or aggregates funds or other assets greater than \$2,000 that they know, suspect or have reason to suspect: 1) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; 2) is designed to evade the requirements of the Bank Secrecy Act, whether through structuring or other means, or 3) serves no business or apparent lawful purpose, and no reasonable explanation for the transaction is known after examining all available facts. See 31 C.F.R. § 1022.320(a)(2).

Most, if not all, illicit CVC mixing activity at or above the SAR filing threshold would be covered by this definition, as bad actors use CVC mixing for the very purpose of evading detection by law enforcement and financial institutions.<sup>18</sup> The information that would be reported in such a SAR includes the amount and type of CVC transferred, the transaction date, identifying information of the relevant customer, and a narrative describing the CVC mixing activity—the very same information required by the NPRM.<sup>19</sup> The only potentially new reporting would come from conduct under the current \$2,000 SAR reporting threshold. But, as explained in more detail below, FinCEN has already determined that any potential benefit coming from this reporting is outweighed by the severe compliance burden it puts on covered entities. The NPRM, therefore, does not fill any existing gap in the BSA reporting rules, but, as explained below, puts enormous burdens on VASPs that will require them to shift resources away from more effective, proactive compliance activities.

Indeed, both the FATF and European Banking Authority (EBA) have recommended that financial institutions address CVC mixing through *existing* SAR reporting procedures. Specifically, in its 2021 Updated Guidance for VASPs, the FATF encouraged the use of risk-based indicators and typologies to inform already existing SAR filing requirements.<sup>20</sup> Further, in its 2020 Report on CVC Red Flag Indicators, the FATF noted that “the mere presence of these features [CVC mixing] in an activity does not automatically suggest an illicit transaction,” and set fourteen indicators that financial institutions should review before concluding that the customer’s use of CVC mixing was for illicit activity.<sup>21</sup> Likewise, the EBA found that potential risks associated with CVC mixing can be mitigated through the use of blockchain analytics, and thus recommended that financial institutions incorporate this technology into their compliance controls—which most, if not all, regulated exchanges are already doing.<sup>22</sup>

To the extent that FinCEN wants VASPs to collect and file more information on transactions that *evade* or *obscure* the SAR filing rule, it can accomplish this more effectively by simply putting out an advisory or alert about CVC mixing trends, typologies, or indicators that

---

<sup>18</sup> The NPRM states that “only a portion of the activity in the CVC ecosystem with exposure to CVC mixing is captured by BSA reporting” but fails to cite the evidence for this statement, nor does the NPRM explain if the lack of reporting is because of non-compliance with existing BSA requirements or an actual regulatory gap. *See* NPRM at 19.

<sup>19</sup> *See* NPRM at 77; FinCEN Form 109.

<sup>20</sup> *See* FATF, *Virtual Assets and Virtual Asset Service Providers*, 88 (Oct. 2021), <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.pdf>.

<sup>21</sup> *See* FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, 9-10 (Sept. 2020), <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf>.

<sup>22</sup> *See* Consultation Paper on Amending Guidelines on ML/TF Risk Factors (EBA Section 21.11)(EBA/CP/2023/11) (31 May 2023) (“CASPs should ensure that systems used by them to identify ML/TF risk associated with individual business relationships, transfers or occasional transactions and to identify suspicious transactions comply with the criteria set out in Title I. In particular, CASPs should ensure that they have adequate transaction monitoring and advanced analytics tools in place . . .”).

help the crypto industry more effectively identify and report under the existing SAR regime—which it has laudably done around cybercrime,<sup>23</sup> ransomware,<sup>24</sup> COVID fraud,<sup>25</sup> human trafficking,<sup>26</sup> sanctions evasion,<sup>27</sup> and other topics. None of these topics—some of which likely pose equal or greater illicit finance risks than CVC mixing—required an expansive new, zero-threshold rule.<sup>28</sup>

Imposing rules like the proposed NPRM in the context of these other illicit finance topics would have led to absurd results, like financial institutions having to report all payments to software companies because of potential cybercrime risk, or having to report all payments to hotels because of a potential human trafficking risk. Instead, FinCEN adopted the more targeted approach of helping focus industry on trends and red flags it was seeing across SAR filings, and then distilled this information and data from law enforcement to aid financial institutions in making even more effective regulatory filings, not making it noisier and more confusing—which is exactly what the NPRM would do.

Furthermore, in publishing an alert on CVC mixing service trends, FinCEN could improve the utility of SAR reporting by doing what it has done in many similar cases in the past: include keyword terms and check-boxes for fast sorting by users of the FinCEN database. For example, a few months ago, FinCEN partnered with the Department of Commerce’s Bureau of Industry and Security (BIS) to issue a joint notice with red flag indicators of export control evasion and highlighting a new SAR key term “FIN-2023-GLOBALEXPORT” for financial institutions to reference when reporting potential efforts by individuals or entities seeking to evade U.S. export controls.<sup>29</sup> Rather than eliminate the SAR threshold for all export activity, FinCEN contributed to industry’s understanding of what should be considered “suspicious”

---

<sup>23</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (2016).

<sup>24</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2021-A004, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (2021).

<sup>25</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2021-A001, Advisory on COVID-19 Health Insurance and Health Care-Related Fraud (2021).

<sup>26</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2020-A008, Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity (2020).

<sup>27</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2022-Alert001, FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts (2022).

<sup>28</sup> As an example of the relatively lower illicit finance risks presented by CVC mixing, in 2022 roughly \$8.9 billion in illicit cryptocurrency transaction volume was associated with sanctioned entities and roughly \$5.9 billion was generated from all types of crypto scams, whereas in 2022 roughly \$1.9 billion processed by CVC mixers came from illicit sources. See Chainalysis, *The 2023 Crypto Crime Report*, 5, 46, 86 (Feb. 2023), [https://go.chainalysis.com/rs/503-FAP-074/images/Crypto\\_Crime\\_Report\\_2023.pdf](https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf).

<sup>29</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2023-NTC2, FinCEN and the U.S. Department of Commerce’s Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls (2023).

indicators for filing under the existing SAR filing regime, and helped improve searchability of the information.<sup>30</sup>

Additionally, FinCEN already has created a “cyber event” field that has options for keywords. In November 2021, FinCEN leveraged this field for an advisory related to ransomware, which provided industry with new information about cybercrime typologies (including CVC mixing technologies), red flags for industry to look at when monitoring transactional activity, and guidance on the most helpful information to include in SARs.<sup>31</sup> FinCEN can simply add a “CVC mixing” keyword to the cyber event field, allowing law enforcement to efficiently search for mixing-related activity—all while avoiding the significant negative impact the NPRM would have on consumers and financial institutions.

**B. Without a minimum threshold for recordkeeping and reporting, the NPRM would impose enormous burdens on VASPs and create opportunities for abuse.**

Unlike SAR reporting, which is set at a \$2,000 threshold and requires identification of possibly suspicious activity, the NPRM would require recordkeeping and reporting on *all* transactions associated with CVC mixing *regardless* of whether there is anything suspicious about them. Almost all bulk recordkeeping and reporting requirements imposed by the BSA on financial institutions include some monetary threshold.<sup>32</sup> FinCEN included these thresholds to avoid mandatory reporting of legitimate, low-value transactions—an obligation that would be unhelpful to FinCEN as would be extremely burdensome to the industry.<sup>33</sup> The same is true here. Without a threshold, VASPs would be required to not only collect large amounts of data on all covered transactions, but would also be required to prepare a narrative on the conduct.<sup>34</sup> Preparing a SAR-like narrative consumes significantly more resources than simply collecting

---

<sup>30</sup> See *id.*; in certain cases, FinCEN has also supplemented advisories with additional information as needed. See, e.g., Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2020-A008, Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity (2020).

<sup>31</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, FIN-2021-A004, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (2021).

<sup>32</sup> See, e.g., 31 C.F.R. §§ 1010.311, 1010.306(c), 1010.410(c) (establishing a (i) \$10,000 threshold for a Currency Transaction Report; (ii) \$10,000 threshold for a Report of Foreign Bank and Financial Accounts; and (iii) \$10,000 threshold for recordkeeping of transactions to recipients outside the U.S.).

<sup>33</sup> See, e.g., Amendments to the Bank Secrecy Act Regulations—Requirement that Money Transmitters and Money Order and Traveler’s Check Issuers, Sellers, and Redeemers Report Suspicious Transactions, 65 Fed. Reg. 13,683, 13,687 (Mar. 14, 2000) (explaining that FinCEN decided to increase the SAR reporting threshold for money services businesses from \$500 to \$2,000 because “reporting suspicious transactions at \$500 would unduly burden the industry given the volume of perfectly legal transactions conducted at or near this dollar amount and would necessarily—given the volume of transactions involved—produce over-reporting . . . [i]n response to these comments, the final rule generally increases the dollar threshold for reporting suspicious transactions to \$2,000. The increase in the reporting threshold to an amount four times the amount originally proposed should help alleviate the concern that the proposed \$500 threshold would cause far too many legitimate transactions to be reported.”).

<sup>34</sup> See NPRM at 77 (requiring a covered financial institution to include a narrative describing the CVC mixing activity associated with covered transactions when reporting such transactions to FinCEN).



data points.<sup>35</sup> Individual compliance analysts would have to review the relevant data and then write extensive narrative reports about the underlying conduct.

While SARs are more useful to law enforcement than other mandatory reporting (such as CTRs, Form 8300s, and CMIRs, which all have \$10,000 thresholds), so-called “defensive” SARs are not. Defensive SARs are filed by financial institutions because of information gaps about the customer or out-of-pattern transactions—not because the underlying conduct appears to be suspicious but rather to achieve technical, check-the-box compliance with the BSA.<sup>36</sup> Unfortunately, defensive SARs account for a significant portion of total SARs filed. FinCEN should be taking steps to combat this trend, which only results in more hay for law enforcement to review—without any concomitant increase in needles.<sup>37</sup> Lacking even a \$2,000 threshold, the NPRM would make defensive SARs an even greater problem.

Financial institutions do not have unlimited resources. They are often forced to choose between check-the-box, defensive reporting and more valuable activities like proactively investigating on and off-platform illicit activity and coordinating investigative efforts with law enforcement.<sup>38</sup> Instead of making VASPs sacrifice useful activities in order to comply with bulk reporting requirements that are not based on suspicious activity, FinCEN should, whenever possible, grant financial institutions discretion in choosing how to best deploy their compliance resources to fight financial crime and assist law enforcement.<sup>39</sup> The NPRM, however, would do the opposite by removing that discretion and imposing strict, zero-threshold bulk data reporting.<sup>40</sup>

---

<sup>35</sup> See, e.g., Agency Information Collection Activities, 85 Fed. Reg. 31,598, 31,608 (proposed May 26, 2020) (noting the significant compliance burdens associated with the drafting, writing, and submitting of SARs by financial institutions).

<sup>36</sup> See Thomson Reuters, *Suspicious Activity Reports Surge: 2023 Filings Expected to Set Another Record*, 3 (2023), <https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2023/06/Suspicious-Activity-Reports-2023.pdf> (“[a]dditionally, the spike in reporting could be attributed to defensive filing, a widely recognized practice in which firms apply overly broad detection criteria to minimize their own risk.”).

<sup>37</sup> See *id.* at 40 (“[l]aw enforcement agencies and professionals have repeatedly voiced concern over increases in defensive filings, while urging firms to include more specific information in SAR filings.”); Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, § 6202, 134 Stat. 3388, 4567 (directing FinCEN to “establish streamlined, including automated, processes to, as appropriate, permit the filing of non complex categories of [suspicious activity reports] that . . . do not diminish the usefulness of the reporting to Federal law enforcement agencies . . .”).

<sup>38</sup> See Aaron Nicodemus, *Financial Institutions Doing More with Less by Outsourcing Compliance* 9 (2023), <https://guidehouse.com/-/media/new-library/industries/financial-services/documents/2023/guidehouse-compliance-week-survey-final.ashx> (noting that limited resources of financial institutions have led to 45% of financial institutions in 2023 outsourcing compliance functions for the purpose of enabling them to “focus on core competencies and better utilize internal resources” to improve compliance efforts, including those related to financial crime).

<sup>39</sup> See, e.g., U.S. Treasury Inspector Gen. for Tax Admin., *The Internal Revenue Service Still Does Not Make Effective Use of Currency Transaction Reports*, Ref. No. 2018-30-076 (Sept. 21, 2018), <https://www.tigta.gov/sites/default/files/reports/2022-02/201830076fr.pdf> (noting that a bulk reporting requirement – filing CTRs – is generally unuseful to the IRS: “[t]he IRS still makes no systemic use of CTR data in examinations” and “the IRS is still not systemically using the CTRs to identify and pursue potentially non compliant individuals.”).

<sup>40</sup> See Financial Times, *US Crypto Clampdown Pushes Exchanges to Go Offshore*, <https://www.ft.com/content/10979399-ba25-45b9-b85d-776c1b75bfea> (last visited Dec. 18, 2023) (noting that stricter US regulation has caused a competitive disadvantage for US exchanges: “US regulators have toughened

The NPRM’s failure to include a threshold would also have enormous negative impacts on consumers. For example, a specific type of privacy attack known as “dusting” occurs when a bad actor sends a small amount of CVC to identify a victim’s larger CVC holdings.<sup>41</sup> Under the NPRM, a dusting attack executed through a CVC mixing service would cause a victim account holder to be automatically reported to law enforcement. Moreover, attackers could spam millions of VASP accounts knowing that those VASPs would then be required to file millions of SAR-like reports on those transactions. The invasion of consumer privacy in this situation would be unparalleled—let alone the insurmountable compliance burden it would create. FinCEN did not address this notable risk in the NPRM.

At the very least, to attempt to remedy these issues, FinCEN should add a filing threshold of \$10,000, which is the same as its other blanket reporting requirements that do not require any identification of suspicious activity, like CTRs, CMIRs, and Forms 8300.

### **C. Bulk data collection and reporting carries minimal benefit for law enforcement and has been expressly discouraged by Congress.**

Congress has made it clear it wants FinCEN to improve the effectiveness of the BSA by streamlining reporting and focusing financial institutions’ efforts on activities that are most useful to law enforcement. A major goal of the Anti-Money Laundering Act of 2020 (“AMLA”) was to “encourage technological innovation and the adoption of new technology . . . to more effectively counter” illicit finance.<sup>42</sup> Further, as Congress described, the AMLA “provides a clear mandate for innovation” and for financial institutions to “effectively . . . test, and adopt leading technologies . . . to track, identify, and report suspicious financial activity.”<sup>43</sup> The NPRM is the opposite of the approach supported by Congress, as it does not seek ways to utilize existing technology held by FinCEN or financial institutions to increase intelligence for law enforcement. Rather, it reverts back to the very bulk data collection and reporting approach that Congress took issue with in the AMLA. Even FinCEN itself has discouraged such bulk data collection and reporting, as FinCEN’s former Director Blanco stated in a congressional hearing that financial institutions should not provide information that is “white noise” or “information for information purposes” to law enforcement.<sup>44</sup>

---

oversight of the digital assets market following the failure of lenders such as Celsius Network and FTX . . . by contrast US crypto exchanges’ offshore rivals have been able to launch products and take market share with less fear of reprisal.”).

<sup>41</sup> See Ciphertrace, *Crypto Dusting*,

<https://ciphertrace.com/glossary/crypto-dusting/#:~:text=Crypto%20Dusting%20is%20a%20cryptocurrency> (last visited Dec. 13, 2023).

<sup>42</sup> See Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, § 6002, 134 Stat 3388, 4547 (2020).

<sup>43</sup> See United States Congress Joint Explanatory Statement of the Committee of Conference on H.R. 6395, at 732, <https://docs.house.gov/billssthisweek/20201207/116hrpt617-JointExplanatoryStatement.pdf>.

<sup>44</sup> See U.S. Senate Comm. On Banking, Hous., and Urban Affairs: Hearing on Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform (Nov. 19, 2018).

Unlike SAR reporting—which is tied to activity being identified as suspicious, and is thus more likely to be useful to law enforcement—bulk data collection and reporting requirements have resulted in a flood of unhelpful data to law enforcement. The value of CTR bulk reporting has been repeatedly questioned, and as many reports have found, large numbers of CTRs go unused and create white noise for law enforcement.<sup>45</sup> Indeed, the Treasury’s Inspector General for Tax Administration has reported that the majority of CTRs are never used.<sup>46</sup> The NPRM’s reporting requirement is like a CTR but even worse—as CTRs at least have a threshold of \$10,000—and would likely create another repository of sensitive information that law enforcement never effectively reviews, let alone uses to build new cases.

**D. Because bulk reporting poses privacy and security risks for consumers who have done nothing wrong, a final rule should at most only require recordkeeping.**

The NPRM’s requirement for covered businesses to *report* extensive personal and financial data of customers (i.e., name, date of birth, address, government ID number, and wallet addresses) creates serious privacy and security risks.<sup>47</sup> Centralizing this highly sensitive information in a single repository—the FinCEN Database—creates a new and strong incentive for hackers to target this information. If hackers obtain this information, they could match a consumer’s actual identity with all of the transactions that he or she has ever made on the blockchain and could use this sensitive information to perpetrate other crimes.<sup>48</sup> Given recent cyberattacks against U.S. government agencies,<sup>49</sup> this privacy and security risk should be of primary concern to FinCEN and cause FinCEN to explain why narrower regulatory alternatives are insufficient before proceeding with this new rule.

---

<sup>45</sup> See U.S. Treasury Inspector Gen. for Tax Admin., *The Accuracy of Currency Transaction Report Data in IRS Systems Should Be Improved to Enhance Its Usefulness for Compliance Purposes*, Ref. No. 2020-30-055 (Sept. 4, 2020), <https://www.oversight.gov/sites/default/files/oig-reports/202030055fr.pdf> (recommending the following actions to remedy deficiencies in the IRS’s use of CTRs: “the IRS [should] use CTR data to systematically identify potentially noncompliant taxpayers and nonfilers, ensure the accuracy of CTR data in the Information Returns Master File, develop processes to verify that data imported are complete and reliable, and ensure the data are accessible to IRS employees.”); see also Courtney J. Linn, *Redefining the Bank Secrecy Act: Currency Reporting and the Crime of Structuring*, Santa Clara Law Review, Volume 50, Number 2, Article 4 at 409 (“Truth be told, there are simply too many currency reports for the government to make full and effective use of them.”).

<sup>46</sup> See U.S. Treasury Inspector Gen. for Tax Admin., *The Internal Revenue Service Still Does Not Make Effective Use of Currency Transaction Reports*, Ref. No. 2018-30-076 (Sept. 21, 2018), <https://www.tigta.gov/sites/default/files/reports/2022-02/201830076fr.pdf> (finding that “[t]he IRS still makes no systemic use of CTR data in examinations” and “the IRS is still not systemically using the CTRs to identify and pursue potentially non compliant individuals.”).

<sup>47</sup> See NPRM at 77 (listing the data elements that must be reported to FinCEN).

<sup>48</sup> See, Jan Henrik Ziegeldorf et al., *Secure and Anonymous Decentralized Bitcoin Mixing*, 80 Future Generation Computer Systems 448-466 (2018) (noting that linking a consumer’s identity to the consumer’s bitcoin wallet address could enable a bad actor to identify the consumer’s complete financial history on the bitcoin blockchain).

<sup>49</sup> See, e.g., Bill Chappell, et al., *What We Know About Russia’s Alleged Hack of the U.S. Government and Tech Companies*, NPR (Dec. 21, 2020), <https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little>.

Rather than requiring covered businesses to report this highly sensitive information to a single repository, a recordkeeping requirement by itself could sufficiently support law enforcement efforts without the significant privacy and security risks presented by the proposed reporting requirement. A recordkeeping-only requirement directing covered businesses to preserve the specified information under the proposed rule would ensure that law enforcement can quickly obtain this information from these institutions through legal process, but only if and when it is actually needed. Importantly, a recordkeeping-only requirement would preserve limited information not otherwise available on the blockchain, but without creating a new centralized stockpile of highly sensitive data.

**E. The NPRM’s failure to consider less restrictive regulatory alternatives is inconsistent with the requirements of the Administrative Procedures Act (APA) and other federal policy directives involving privacy, security, and de-risking.**

The APA demands that federal agencies do not take actions that are either arbitrary or capricious.<sup>50</sup> To satisfy this requirement, a federal agency must provide an explanation based on actual evidence that is beyond a conclusory statement and justifies the action at issue.<sup>51</sup> Importantly, a federal agency’s action is arbitrary and capricious when the agency fails to explain why less restrictive regulatory alternatives to the action at issue are insufficient.<sup>52</sup> In this case, there are a number of less restrictive regulatory alternatives to meet the NPRM’s objectives (e.g., issuing guidance to enhance the effectiveness of the existing SAR regime, establishing a minimum dollar threshold, and relying on recordkeeping rather than reporting). FinCEN must explain why these alternatives are insufficient to satisfy the NPRM’s stated objectives.

Further, the NPRM’s failure to consider less restrictive regulatory alternatives encourages de-risking, which is contrary to federal policy directives. De-risking is the practice of financial institutions mitigating regulatory risk by terminating or restricting business relationships indiscriminately with broad categories of clients rather than doing so in a targeted manner.<sup>53</sup> The U.S. Treasury recently stated that de-risking undermines the BSA because it is “not consistent with the risk-based approach that is the cornerstone of the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) regulatory framework for U.S. financial institutions . . .” and compromises several key policy objectives by, for example, hampering remittances and preventing underserved communities from efficiently accessing the financial system.<sup>54</sup> The NPRM’s expansive definitions (which mandate suspicionless, zero-threshold reporting) and the breadth of legitimate activity it would cover are likely to overwhelm the available resources of many covered businesses in both personnel and cost (as discussed in Section II.B). This would encourage covered financial institutions to de-risk activities related to CVC and therefore undermine federal policy goals opposed to de-risking.

---

<sup>50</sup> See 5 U.S.C. § 706(2)(A).

<sup>51</sup> See *United States v. Dierckman*, 201 F.3d 915, 926 (7th Cir. 2000) (quoting *Bagdonas v. Dep’t of the Treasury*, 93 F.3d 422, 426 (7th Cir. 1996)) (“[t]he agency’s decision ‘need not include detailed findings of fact but must inform the court and the petitioner of the grounds of the decision and the essential facts upon which the administrative decision was based.’ . . . [t]his means that on the administrative record the decision must have a rational basis.”).

<sup>52</sup> See *Cin. Bell Tel. Co. v. FCC*, 69 F.3d 752, 761 (6th Cir. 1995) (invalidating the FCC’s proposed rule because “the FCC has not explained why less restrictive, yet easily administered rules . . . fail in light of its stated objectives. The FCC’s conclusory statements . . . wholly fail to provide a reasoned explanation as to why the less restrictive alternatives described above are insufficient.”); *Motor Vehicle Mfrs. Ass’n v. State Farm Mutual Auto. Ins. Co.*, 463 U.S. 29, 48, 103 S.Ct. 2856 (1983) (holding that an “alternative way of achieving the [stated] objectives . . . should have been addressed and adequate reasons given for its abandonment”).

<sup>53</sup> See U.S. Dep’t of the Treasury, *The Department of the Treasury’s De-risking Strategy*, 1 (Apr. 2023), [https://home.treasury.gov/system/files/136/Treasury\\_AMLA\\_23\\_508.pdf](https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf).

<sup>54</sup> See *id.*

In addition, the NPRM undermines FinCEN’s own policy directives to apply a technology neutral regulatory approach and encourage data privacy, protection and security. FinCEN has consistently avoided targeting a particular kind of technology to mitigate the risk of undermining financial innovation. In other words, FinCEN has been “technology neutral” in its regulatory efforts for the purpose of ensuring its rules can cover a range of activity regardless of the kind of innovations used to facilitate such activity.<sup>55</sup> For example, FinCEN has referenced this technology neutral approach when explaining that certain CVC-related activity is subject to the money transmitter regime under the BSA: “because we are technology neutral, we can say with complete clarity that for AML/CFT purposes, it should be understood that transactions in stablecoins, like any other value that substitutes for currency, are covered by our definition of ‘money transmission services.’”<sup>56</sup>

As discussed in Section III.A, this NPRM takes the opposite approach of defining technology—extremely broadly—summarily labeling it “high risk.” This is a substantial deviation from FinCEN’s traditional activity-based, technology-neutral regulatory approach.

Further, by discouraging privacy-security technology for payments, the NPRM is at odds with actions by FinCEN itself, to encourage data privacy, protection, and security. Burdensome reporting requirements directed at an expansive technology-defined category are likely to undermine a critical area of privacy-preserving cryptography and technological innovation of which FinCEN itself has recognized the value and encouraged the development.<sup>57</sup> FinCEN has repeatedly acknowledged—as it rightly does at times in the NPRM—that privacy is part of the “security” and “resilience” of our financial system, and a “building block for protecting” it.<sup>58</sup> The

---

<sup>55</sup> See Testimony of Thomas P. Ott, Associate Director, Enforcement Division, before the House Committee on Financial Services, <https://www.fincen.gov/news/testimony/testimony-thomas-p-ott-associate-director-enforcement-division-house-committee> (“[t]he definition of money transmission is technology neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another person or location is regulated under the BSA.”); Prepared Remarks of James H. Freis, Jr., Director, Financial Crimes Enforcement Network 1-2, <https://www.fincen.gov/sites/default/files/shared/20100901.pdf> (“the framework for money transmission . . . is an activity-based test . . . [t]his is technology neutral and is meant to be adaptable to a range of products, whether tied to a plastic card, an internet system, or a mobile phone network.”).

<sup>56</sup> See Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-chainalysis-blockchain-symposium#:~:text=FinCEN%27s%20technology%20neutral%20approach%20also,grin%2C%20dash%2C%20and%20others>.

<sup>57</sup> See, e.g., FinCEN to Host Innovation Hours Program Workshop on Privacy Enhancing Technologies, <https://www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-privacy-enhancing-technologies> (describing FinCEN’s Innovation Hours Program as “an example of FinCEN’s ongoing dedication to advancing the integrity and innovative strength of the U.S. financial system, which includes balancing transparency and accountability with the important principles of privacy and security . . .”).

<sup>58</sup> See *id.*; FinCEN Acting Director’s Statement Regarding U.S., U.K. Collaboration on Prize Challenges to Accelerate Development and Adoption of Privacy-Enhancing Technologies, <https://www.fincen.gov/news/news-releases/fincen-acting-directors-statement-regarding-us-uk-collaboration-prize-challenges> (“FinCEN is pleased to support this important initiative to advance the development of a building block for protecting the U.S. financial system from illicit finance.”).

NPRM’s expansive targeting of privacy enhancing technology is strikingly at odds with protecting American people and our financial system that is fundamental to FinCEN’s mission.

Finally, given the broad scope of new information that would be collected and processed under the NPRM, FinCEN should explain how it will comply with its information security obligations. Specifically, FinCEN has information security obligations under The Privacy Act of 1974, which requires federal agencies that decide to establish or make changes to a system of records to notify the public by a notice published in the Federal Register identifying “the categories of records”, “the categories of individuals on whom records are maintained”, and “each routine use of the records” among other items.<sup>59</sup> Further, the E-Government Act of 2002 imposes information security obligations on FinCEN by requiring that agencies conduct “privacy impact assessments” prior to procuring or developing government data systems.<sup>60</sup> The NPRM fails to address, entirely, the data collection notice requirement under the Privacy Act as well as the privacy impact assessment required by the E-Government Act. Accordingly, especially considering FinCEN’s well-known resource limitations, FinCEN should provide the public an opportunity to assess and comment upon the sufficiency of the information security controls required under the Privacy Act and the E-Government Act—and FinCEN’s resources to implement them—before finalizing the NPRM.

**III. The NPRM’s definitions are extraordinarily broad, making them unworkable for regulated VASPs and covering a scope of activity far beyond what FinCEN claims to be high risk.<sup>61</sup>**

**A. The NPRM’s definition of “CVC mixing” would cover a scope of crypto activity far broader than the identified risks FinCEN is seeking to address and without any evidence this broader activity actually poses an illicit finance risk.**

The NPRM’s definition of “CVC mixing” goes far beyond the actual risks the NPRM articulates, which are focused almost entirely on custodial CVC mixer services, as the NPRM broadly references CVC mixing as services “intended to obfuscate transactional information.”<sup>62</sup> Rather than limiting its scope to custodial CVC *mixer services*, this NPRM definition would cover an astoundingly broad range of CVC *mixing activity* that is not primarily designed to obfuscate transactional information and does not pose an illicit finance risk—including but not

---

<sup>59</sup> See 12 U.S.C. § 552a(e)(4).

<sup>60</sup> See E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002).

<sup>61</sup> This section responds to the NPRM’s general request for input, as well as the following questions: “1. Does FinCEN accurately account for the burden and impact of this proposed rule when a covered financial institution knows, suspects, or has reason to suspect a transaction involves CVC mixing?”; “7. Are the due diligence requirements appropriately scoped in this proposed rule?”.

<sup>62</sup> See NPRM at 7.

limited to “pooling,”<sup>63</sup> “splitting,”<sup>64</sup> “programmable or algorithmic code,”<sup>65</sup> “single-use wallets,”<sup>66</sup> “exchanges between types of CVC,”<sup>67</sup> and “user-initiated delays.”<sup>68</sup> As explained below, the NPRM fails to provide any significant evidence that this broader category of CVC *mixing activity* poses an illicit finance risk that warrants a new proposed rule.

As an initial matter, the definition of “CVC mixing activity” would cover almost all CVC mixing activity except for one category that is explicitly exempted from the NPRM—use of internal protocols by VASPs to execute transactions assuming certain recordkeeping requirements are met.<sup>69</sup> There is otherwise no limiting principle for the proposed definitional scope of anything that “obfuscates the source, destination, or amount” involved in a transaction.<sup>70</sup> This means that any smart contract, decentralized exchange, wallet software, or cross-chain bridge could be covered if even a collateral but not intended effect is to obfuscate any information about the source, destination, or amount of the transaction. Even the most basic direct transaction between one CVC wallet to another could be covered if the transactors are, for example, creating new wallets just for that transaction. The de facto result of this limitless definition is that regulated exchanges would be forced to retain records and file SAR-like reports on any transaction that is not received directly from or sent directly to another regulated exchange. But, as explained herein, the NPRM lacks almost any justification for this broad definition.

In Section IV—which serves as the factual justification for the proposed rule—the NPRM makes scant reference to any specific illegal uses of CVC mixing activity other than in the narrow context of custodial CVC mixer services. Indeed, almost every substantive reference is to illegal custodial CVC mixer services, not the broader category of CVC mixing activity that the NPRM nonetheless uses for its definition. And at times, the NPRM appears to inconsistently use these different terms, conflating custodial CVC mixer services with the much broader category of CVC mixing activity. In addition, many of the citations to third-party research conducted on CVC mixing fails to support the factual claims asserted in the NPRM and, sometimes, even directly contradict Section IV of the NPRM, as explained below. These major

---

<sup>63</sup> See *id.* at 8 (noting that pooling “involves combining CVC from two or more persons into a single wallet or smart contract . . .”).

<sup>64</sup> See *id.* at 8-9 (noting “[t]his method involves splitting a single transaction from sender to receiver into multiple, smaller transactions, in a manner similar to structuring . . .”).

<sup>65</sup> See *id.* at 9 (noting programmable or algorithmic code “involves the use of software that coordinates two or more persons’ transactions together . . .”).

<sup>66</sup> See *id.* at 9 (noting “[t]his method involves the use of single-use wallets, addresses, or accounts—colloquially known as a “peel chain”—in a series of unnatural transactions . . . volumetrically increasing the number of involved transactions . . .”).

<sup>67</sup> See *id.* at 9-10 (noting “[t]his method involves exchanges between two or more types of CVC or other digital assets—colloquially referred to as “chain hopping” . . .”).

<sup>68</sup> See *id.* at 10 (noting user-initiated delays involve “the use of software, programs, or other technology that programmatically carry out predetermined timed-delay of transactions by delaying the output of a transaction . . .”).

<sup>69</sup> See *id.* at 75-76.

<sup>70</sup> See *id.*



research deficiencies and errors make the NPRM a flawed document on which to base any new proposed rule.

Looking closely at Section IV of the NPRM, there are only a few factual citations referencing CVC mixing as a serious illicit finance risk,<sup>71</sup> and FinCEN has not cited a single publicly available example of CVC mixing (other than in the context of CVC mixer services, i.e. platforms specifically designed to provide obfuscation services)<sup>72</sup> being used as a significant tool for money laundering. For example, the NPRM asserts that CVC mixing is “a prevalent money laundering typology for the top 10 ransomware strains[,]” yet the citation to a Chainalysis research article does not support this claim.<sup>73</sup> That article does not once reference CVC mixing activity in the broad sense but instead has a single reference to “mixers” sending funds to Moscow City CVC businesses, and yet, the actual data shows that throughout 2021, transactions involving addresses Chainalysis considers “risky” (which include mixers), actually dropped significantly.<sup>74</sup>

Similarly, the NPRM claims that certain European law enforcement takedowns “demonstrate the international character of CVC mixing transactions,” but every one of those takedowns involved custodial mixer services, not the more broadly defined CVC mixing activities.<sup>75</sup> Further on, the NPRM claims that non-state hackers “commonly use CVC mixing services to launder their proceeds from large scale heists,” but the only specific reference was to the mixer service Tornado Cash.<sup>76</sup> The NPRM also claims that state actors like North Korea use CVC mixing as part of their money laundering, and cites FinCEN’s imposition of a Special Measure against North Korea in 2016 to support this claim. But that public notice does not make a single reference to CVC, let alone CVC mixers or mixing activity.<sup>77</sup>

The NPRM also refers to a Chainalysis research article on North Korea’s CVC money laundering techniques, but that article does not make any explicit references to CVC mixing

---

<sup>71</sup> See, e.g., *id.* at 14, fn. 32; 18 fn. 55, 56.

<sup>72</sup> The majority of the CVC mixer services referenced in the NPRM are custodial CVC mixer services, and some of them were custodial and later became non-custodial, such as Tornado Cash, which was custodial during its first year of operating (2019-2020).

<sup>73</sup> See NPRM at 14; Chainalysis, *Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity*, <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/> (last visited Dec. 15, 2023).

<sup>74</sup> See Chainalysis, *Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity*, <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/> (last visited Dec. 15, 2023) (showing a significant drop in transactions from first half of 2021 to second half of 2021 involving addresses Chainalysis considers “risky”, which include mixers, although the article does not breakdown how much of these “risky” transactions were from mixers versus high-risk centralized exchanges).

<sup>75</sup> See NPRM at 15-16.

<sup>76</sup> See *id.* at 16.

<sup>77</sup> See *id.* at 16-17, fn. 43.

activities in the context of money laundering techniques. It instead refers only to CVC “mixers.”<sup>78</sup> Notably, that Chainalysis article references North Korea’s use of decentralized exchanges (DEXs), but not as a money laundering tool. Instead, the article notes that DEXs allowed North Korea to convert stolen altcoins to ERC-20 tokens that were more convertible to cash.<sup>79</sup> In other words, DEXs were used by North Korea not to launder funds, i.e. to make their source, nature, ownership, or control more difficult to ascertain, but instead to make it easier for North Korea to cash out through traditional financial institutions. This is not an obfuscation issue but rather one of sanctions enforcement that the NPRM would not fix.

These research errors continue throughout Section IV of the NPRM. Another example is where the NPRM claims that FinCEN’s 2021 Financial Trend Analysis (FTA) on Ransomware shows that prevalent money laundering typologies of threat actors have included “avoiding reusing wallets, using CVC mixing services, and ‘chain hopping.’”<sup>80</sup> However, according to the FTA, bitcoin sent to mixers from wallet addresses used for ransomware-related payments by the top 10 most common ransomware variants accounted for only *one percent* of all bitcoin sent from such addresses.<sup>81</sup>

On the following page, the NPRM asserts without support that ransomware actors have used chain hopping and other CVC techniques to layer funds through multiple wallet addresses and setting up new wallets for each ransomware attack.<sup>82</sup> But the NPRM fails to analyze whether those CVC transactional techniques had any impact whatsoever on law enforcement’s ability to trace the funds. In other words, a bad actor’s use of a technique does not necessarily mean that the technique is effective and creates a regulatory gap. According to TRM Labs, a blockchain analytics firm cited by the NPRM, current technology allows investigators to “trace through bridges in the click of a button and [] visualize the movement of funds from one blockchain to

---

<sup>78</sup> See NPRM at 17 fn. 46; Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, <https://www.chainalysis.com/blog/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/> (last visited Dec. 15, 2023) (noting that DPRK has used DeFi platforms to convert stolen tokens into more liquid tokens, unlike mixer services, which DPRK has used to obfuscate the source and ownership of the funds).

<sup>79</sup> See Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, <https://www.chainalysis.com/blog/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/>

<sup>80</sup> See NPRM at 18, fn. 56.

<sup>81</sup> See Financial Crimes Enforcement Network, U.S. Dep’t of the Treasury, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*, 12 (Oct. 2021), [https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis\\_Ransomware%20508%20FINAL.pdf](https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf)

<sup>82</sup> See NPRM at 19-20.

another . . . ”.<sup>83</sup> This undermines the NPRM’s claim that CVC mixing poses such a serious obfuscation threat that FinCEN must issue an expansive, burdensome new bulk data collection rule to address it.

Taken as a whole, the NPRM fails to support its claim that CVC mixing activity (as broadly defined in the NPRM) poses a significant money laundering risk, and in fact, the NPRM seems to ignore evidence to the contrary. There is little to no evidence or basis in the proposed rule to cover the broader category of CVC mixing activity, i.e. pooling, chain hopping, smart contracts, etc.—as opposed to a definition more narrowly focused only on custodial CVC mixer services.

**B. The exemption on transactions with compliant financial institutions is unworkable because it would put significant counterparty due diligence requirements on all VASPs, and also appears to exempt transactions with custodial CVC mixer services—the only entities on which Section IV of the NPRM seems focused.**

As described above, Section IV of the NPRM appears to focus squarely on the problem of custodial mixer services, in which a centralized entity takes custody of customer CVC, pools those funds, converts them into another form of CVC, and then sends the funds to a designated recipient address. But, because these entities take custody of customers’ CVC and then transmit that CVC to another destination, they typically qualify as MSBs under the BSA—including being subject to FinCEN enforcement actions for non-compliance.<sup>84</sup> It also means that, under the current NPRM, these entities are actually exempted from the NPRM’s definition of CVC mixing and the new proposed requirements, because they use “internal protocols or processes to execute transactions by [MSBs],” provided that they “preserve records of the source and destination of CVC transactions . . . and provide such records to regulators and law enforcement . . . ”.<sup>85</sup>

Several issues arise from this apparent exemption of custodial mixer services. First, if the core illicit finance concern identified in the NPRM is custodial mixer services, the NPRM is on its face ineffective because it would not mandate reports on transactions with those very institutions. As explained above, the NPRM’s risk assessment focuses almost entirely on custodial mixer services, not the broader category of CVC mixing activity that the NPRM fails to tie to any notable illicit finance risks. It makes no sense to punish covered businesses (and their

---

<sup>83</sup> See TRM Labs, *TRM Phoenix Solves Crypto Investigators’ ‘Chain-Hopping’ Problem*, <https://www.trmlabs.com/post/trm-phoenix-solves-crypto-investigators-chain-hopping-problem> (last visited Dec. 15, 2023); Chainalysis, *Storyline*, <https://www.chainalysis.com/chainalysis-storyline/> (last visited Dec. 15, 2023) (offering a similar blockchain analytics tool); Elliptic, *Typologies in Focus: The Threat of Cross-Chain Crime*, <https://www.elliptic.co/blog/typologies-in-focus-the-threat-of-cross-chain-crime> (last visited Dec. 15, 2023) (offering a similar blockchain analytics tool).

<sup>84</sup> See NPRM at 32 (citing 31 C.F.R. § 1010.100(ff)(5)(A)).

<sup>85</sup> See *id.* at 76.

customers) for transacting with the broader category when the only identified risk rests with the smaller category of custodial mixer services.

FinCEN notes that this exemption applies only to compliant MSBs—and thus potentially not non-compliant offshore CVC mixer services. But this then begs the question of how covered exchanges could ever know if a domestic or foreign MSB counterparty is compliant with its legal obligations? The NPRM does not answer this question. Instead, it simply states that the exemption applies to “known VASPs [] that are positioned to appropriately respond to inquiries by law enforcement . . .”.<sup>86</sup> But to know this, a covered business would have to conduct extensive due diligence on all counterparties to determine if they fall within this exemption—a de facto high risk designation for all VASPs that is unfeasible, impractical, and unjustified. Nor is it a burden properly addressed in the NPRM.

FinCEN could further clarify and narrow the scope of the proposed rule only to require reports on custodial mixer services. But the NPRM explicitly acknowledges that this would impose an undue burden on covered businesses by requiring reports on information when covered businesses are already “taking appropriate steps to ensure information is being retained as prescribed by law.”<sup>87</sup> The issues with this exemption only underscore the broader problems underlying the NPRM—both the factual basis on which it relies and the effectiveness of the new proposed requirements to address any real risk.

---

<sup>86</sup> *See id.* at 31.

<sup>87</sup> *See id.* (the NPRM states that this exception was crafted “to avoid imposing undue burden on covered businesses, provided they are also taking appropriate steps to ensure information is being retained as prescribed by law.”).

**C. Without clear limiting principles, the NPRM’s coverage over any transaction that an exchange “knows, suspects, or has reason to suspect involves CVC mixing” is too vague for exchanges to implement and would likely result in a de facto high risk designation for all CVC transactions.**

The NPRM’s recordkeeping and reporting requirements would apply to any transaction that a covered business “knows, suspects, or has reason to suspect involves CVC mixing . . .”<sup>88</sup> But the NPRM does not provide any guidance, let alone a limiting principle, as to what transactions are covered by this definition. Specifically, this definition on its face may cover transactions not just directly to or from CVC mixing, but also transactions with historical connections to CVC mixing—one, two, three or more steps removed. So, CVC that can be historically traced via blockchain analytics to a certain CVC mixer service may be deemed permanently high risk because of that historical connection.

This would punish innocent users who by chance come into possession of CVC that months or years earlier touched a CVC mixer service. It also means that exchanges would have to conduct blockchain analysis on every incoming or outgoing transaction to look for these historical connections—which without a limiting principle could include a significant percentage of all CVC transactions.<sup>89</sup> This is a burden not properly addressed or even considered by the NPRM. To remedy this issue, the NPRM must include a temporal limiting principle that makes covered business responsible only for identifying transactions *directly* sent to or received from CVC mixing services.

Besides not having a temporal limiting principle, i.e. direct transactions only, the NPRM should also include a de minimis exception so that CVC assets are not permanently tainted by small interactions with CVC mixing. This issue can arise if a de minimis amount of CVC is sent via a mixer service to a wallet that contains funds that have not interacted with a mixer service. Along these same lines, attackers using dusting techniques could make the wallets of innocent CVC owners subject to the NPRM’s privacy-infringing mandates through no fault of their own (as discussed above).<sup>90</sup>

The NPRM simply fails to explain if the “involved” CVC mixing definition covers commingled assets, and, if so, how it can justify enhanced reporting requirements on funds that

---

<sup>88</sup> See *id.* at 32.

<sup>89</sup> For example, CVC mixers processed roughly \$8 billion in CVC transactions in 2022, which amounts to roughly 1% of Coinbase’s total CVC trading volume in 2022. See Chainalysis, *The 2023 Crypto Crime Report*, 46 (Feb. 2023), [https://go.chainalysis.com/rs/503-FAP-074/images/Crypto\\_Crime\\_Report\\_2023.pdf](https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf) (finding that CVC mixers processed roughly \$8 billion of CVC in 2022); The Block, *Coinbase’s Total Volume*, <https://www.theblock.co/data/crypto-markets/public-companies> (last visited Dec. 16, 2023) (finding that Coinbase’s total trading volume in 2022 was roughly \$830 billion).

<sup>90</sup> See Office of Foreign Assets Control, U.S. Dep’t of the Treasury, Frequently Asked Question #1078, <https://ofac.treasury.gov/faqs/updated/2022-11-08> (discussing dusting attacks against wallets of innocent CVC owners in connection with OFAC’s broad designation of all Tornado Cash smart contracts).

were not exposed to the obfuscation techniques at issue in the NPRM (and the increased reporting burden it would create for covered businesses).<sup>91</sup> As explained above, Coinbase recommends that FinCEN both adopt the \$10,000 reporting threshold described above—aligned with the other FinCEN reporting that does not require any suspicious activity—to help mitigate this issue while also explicitly exempting any non-mixed CVC funds in a commingled wallet.

**IV. Before implementing any part of the proposed rule, FinCEN should provide a “sunrise” roadmap for which industry can provide feedback on how FinCEN and industry will implement any new rule.<sup>92</sup>**

The NPRM establishes extensive requirements concerning the collection, storage and transmission of highly sensitive personal information that, once linked to a public wallet address, could reveal all of an individual’s blockchain transactions. Significant aspects of this new, major data collection and reporting regime are not addressed in the NPRM and need to be described in detail for industry’s feedback, otherwise there is significant risk of mishandling of large volumes of data. As with prior rulemakings for new information collections (e.g. SARs, the Travel Rule, Foreign Bank Account Reports, and CTRs), FinCEN should provide draft forms and guidance for industry to provide feedback and questions, with consensus reached before any rule was finalized. Given these considerations, FinCEN should provide a significant sunrise period of at least one year, but likely longer, before issuing a final rule.

For reference, when the Travel Rule, which requires far less complex and wide-ranging data than contemplated here, was issued in 1995,<sup>93</sup> there were successive—sometimes 2-year at a time—“safe harbors,” amendments, and exceptions provided in 1996,<sup>94</sup> 1998,<sup>95</sup> and ultimately concluding in 2003,<sup>96</sup> providing an 8-year sunrise period before full implementation was expected or enforced. FinCEN acknowledged industry concerns that the new rule “will require significant resources and would likely involve diverting programming time away from more

---

<sup>91</sup> In other contexts, the legitimate portion of commingled assets are set aside from the illegitimate portion, such as with asset forfeiture, in which the forfeiture of the legitimate portion of commingled assets may constitute a violation of the Excessive Fines Clause of the Eighth Amendment if grossly disproportionate to the gravity of the defendant’s offense. *See, e.g., United States v. Castello*, 611 F.3d 116, 120-21 (2nd Cir. 2010) (establishing that a court must enter a forfeiture order equal to the maximum authorized by statute less the minimum amount necessary to render the total amount not grossly disproportionate to the offense in accordance with the Eighth Amendment).

<sup>92</sup> This section responds to the NPRM’s general request for input, as well as the following question: “1. Does FinCEN accurately account for the burden and impact of this proposed rule when a covered financial institution knows, suspects, or has reason to suspect a transaction involves CVC mixing?”

<sup>93</sup> *See* Conditional Exceptions to Bank Secrecy Act Regulations Relating to Orders for Transmittals of Funds by Financial Institutions, 63 Fed. Reg. 3640, 3640 (Jan. 26, 1998).

<sup>94</sup> *See id.* at 3641.

<sup>95</sup> *See id.* at 3642.

<sup>96</sup> *See* Notice of Expiration of Conditional Exception to Bank Secrecy Act Regulations Relating to Orders for Transmittals of Funds by Financial Institutions, 68 Fed. Reg. 66,708, 66,708 (Nov. 28, 2003).

urgent programming needs.”<sup>97</sup> In providing another round of relief, FinCEN recognized “computer programming problems in the banking and securities industries” as hurdles to implementing the new (and far more basic) reporting requirements and invited comments as to whether some terms of the “exception should be permanently incorporated into the Travel Rule.”<sup>98</sup> Similarly, a FinCEN rule amending the process by which financial institutions may exempt certain transactions from reporting under the currency transaction reporting regime provided a two-year compliance period, noting that banks would need “ample time . . . to move from the prior administrative exemption system to the reformed system” and solve other technical difficulties.<sup>99</sup>

Further, as part of this sunrise period, FinCEN can also consider implementing an extended temporary exemption for affected financial institutions, which FinCEN has done before.<sup>100</sup> FinCEN’s rationale for doing so was that it should first have time to develop an adequate understanding of the affected entities before making a final rule. Without this time, FinCEN could end up with “poorly conceived regulations that impose unreasonable regulatory burdens with little or no corresponding anti-money laundering benefits.”<sup>101</sup> FinCEN should take a similarly cautious and practical approach to understanding affected entities in the context of CVC mixing activity before subjecting them to new rules.

The current proposal does not address any of these issues, which will require meaningful opportunity for industry to provide comment in a new draft proposal.

\* \* \*

---

<sup>97</sup> See Conditional Exceptions to Bank Secrecy Act Regulations Relating to Orders for Transmittals of Funds by Financial Institutions, 63 Fed. Reg. 3640, 3641 (Jan. 26, 1998).

<sup>98</sup> See Extension of Grant of Conditional Exception to Bank Secrecy Act Regulations Relating to Orders for Transmittal of Funds by Financial Institutions, 66 Fed. Reg. 32,746, 32,746 (Jun. 18, 2001).

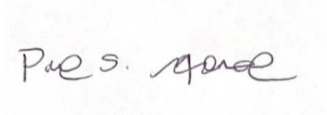
<sup>99</sup> See 63 Fed. Reg. 50,147, 50,155 (Sept. 21, 1998) (noting that FinCEN extended the initial implementation date due to these technical difficulties: “[i]n light of these comments, the transition period stated in the Notice—that, in effect, provides banks until the end of the calendar year 1999 to make the transition to the reformed system—has been extended in the final rule to July 1, 2000. Provided that banks comply with the transition period set forth in the final rule, they may treat a customer as exempt under either the prior administrative exemption rules or the reformed exemption procedures . . . during the transitional period.”).

<sup>100</sup> See 67 Fed. Reg. 21,110, 21,111 (Apr. 29, 2002) (noting that “Treasury and FinCEN are exercising the authority under BSA section 5318(a)(6) to temporarily exempt all other financial institutions from the requirement in section 5318(h)(1) that they establish anti-money laundering programs . . . [t]he temporary exemption . . . applies to dealers in precious metals, stones or jewels; pawnbrokers; loan or finance companies . . .”).

<sup>101</sup> See *id.* at 21,112.

Coinbase appreciates the opportunity to work with Treasury to develop sound, effective regulation. We encourage Treasury to consider the serious concerns we have outlined above with the NPRM, and work with industry to develop novel and collaborative approaches to combating illicit finance, through which Treasury can make regulatory and law enforcement efforts more effective while also ensuring that the United States remains at the forefront of innovation in financial services.

Sincerely,

A handwritten signature in black ink, appearing to read "Paul Grewal", is centered on a light gray rectangular background.

Paul Grewal  
Chief Legal Officer  
Coinbase