



January 22, 2024

Docket No. FINCEN-2023-0016

VIA ELECTRONIC SUBMISSION

Andrea Gacki  
Financial Crimes Enforcement Network  
P.O. Box 39  
Vienna, VA 22183

RE: Paradigm Operations LP Comment Regarding  
Notice of Proposed Rule Making (FINCEN-2023-0016)

Dear Ms. Gacki:

Paradigm Operations LP (“Paradigm”) appreciates the opportunity to comment on the October 19, 2023, Notice of Proposed Rule Making (“NPRM”) entitled “Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern” (the “Proposed Rule”).

**I. Introduction**

Paradigm is an American research-driven investment firm, based in San Francisco, that focuses on crypto and related technologies at the frontier. Paradigm takes a hands-on approach to help the projects it invests in reach their full potential, from the technical (mechanism design, security, engineering) to the operational (recruiting, go-to-market, legal and regulatory strategy).<sup>1</sup> Paradigm believes that a flourishing and innovative crypto technology ecosystem depends on sound and sensible regulation and that industry must work in collaboration with the U.S. and other governments in this effort. Paradigm has a track record of proactive engagement with the U.S. government, including through its Policy Director serving

---

<sup>1</sup> More information about Paradigm is available at <https://www.paradigm.xyz>.

Andrea Gacki  
January 22, 2024  
Page 1

as a member of the Commodity Futures Trading Commission's Technology Advisory Committee and Subcommittee on Digital Assets and Blockchain Technology,<sup>2</sup> and its filing of various comment letters to rulemaking proposals by the Securities and Exchange Commission, Internal Revenue Service, and Consumer Financial Protection Bureau.<sup>3</sup>

Paradigm shares FinCEN's concern that crypto, like any technology, has the potential to be abused by bad actors. However, Paradigm respectfully submits that the Proposed Rule is not the appropriate tool to address this concern and implementation in its current form would have negative effects for the national security interests of the United States and drive the development of blockchain technology offshore. FinCEN already has the tools needed to address the risks presented by the illicit use of virtual currency mixers.

***The Proposed Rule misdiagnoses the source of risk, focusing on general application technology, instead of bad actors themselves.*** While the Proposed Rule attempts to tackle the legitimate risk of bad actors using virtual currency mixers to obscure ill-gotten gains and fund terrorism and other illicit activities, it misplaces the onus of responsibility for the risk. Rather than focusing reporting requirements on the bad actors that exploit otherwise legitimate technologies, the rule focuses on a broad swath of rapidly developing technologies that may, for legitimate reasons and in the course of normal operations, anonymize the source, destination, or amount of a transaction. These types of technologies and activities have many legitimate applications and should not be broadly considered to be "of primary money laundering concern."

***The Proposed Rule is a blunt instrument that would create an undue regulatory burden on the development of blockchain technology in the United States.*** The Proposed Rule seeks to impose upon financial institutions onerous reporting rules on transactions involving any person, group, service, code, tool, or function that anonymizes the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used, and for whatever reason. As written, the Proposed Rule goes well beyond creating an enhanced reporting requirement related to services traditionally understood to be virtual currency mixers, such as Blender.io and Tornado Cash. Rather the Proposed Rule would, in effect, create a general enhanced reporting requirement for crypto transactions, touching on activities and services completely unrelated to virtual

---

<sup>2</sup> See Subcomm. on Dig. Assets & Blockchain Tech., Tech. Advisory Comm., U.S. Commodity Futures Trading Comm'n, *Decentralized Finance* (Jan. 8, 2024).

<sup>3</sup> See Paradigm, *Policy Lab at Paradigm*, <https://policy.paradigm.xyz/actions> (last visited Jan. 19, 2024).

Andrea Gacki  
January 22, 2024  
Page 2

currency mixing and that do not raise inherent money laundering and terrorist financing risks. These reporting requirements would create a regulatory burden for regulated financial intermediaries dealing with crypto entrepreneurs that would ultimately drive the development of crypto offshore.

To the extent that FinCEN decides to pursue the Proposed Rule, the definitions of “CVC mixing” and “CVC mixer” should be narrowed to focus on specific and clearly defined activities.

*There are existing tools that address the FinCEN-identified risks in a more targeted and effective manner.* Today, FinCEN’s suspicious activity report (“SAR”) regime requires financial institutions to identify and report transactions potentially linked to illicit finance and terrorism, among other activities. The SAR reporting system is robust and far reaching and remains the best tool to address FinCEN’s concerns around virtual currency mixers. To aid financial institutions in their reporting obligations, FinCEN could increase industry guidance regarding red flags and other specific indicators of suspicious activity relating to money laundering and terrorist financing presented by virtual currency mixers. Guidance can be supplemented, as may be appropriate, by the designation of specific bad actors under FinCEN’s Section 311 authorities. By leveraging the SAR reporting regime and issuing targeted industry guidance, FinCEN can collect more useful, tailored, and actionable information without overly burdening financial institutions.

**II. Technologies that have the effect of anonymizing the source, destination, or amount of virtual currency transactions are not inherently problematic and should not be considered “of primary money laundering concern.”**

Paradigm shares FinCEN’s concern about the abuse of technology by illicit actors, including their use of virtual currency mixing services. Recognizing the critical importance of combating criminal abuse of the crypto ecosystem, Paradigm has launched various public security initiatives, including ones aimed at facilitating information sharing between industry and law enforcement bodies,<sup>4</sup> and plays a key role in responding to active exploits of crypto protocols. FinCEN rightly identifies that certain bad actors have used virtual currency mixers to launder criminal proceeds and facilitate ransomware and darknet markets payments. These criminals not only threaten the safety and security of the U.S. financial system, but they also

---

<sup>4</sup> See, e.g., Sebastian Sinclair, *DeFi gets a “SEAL” Team as White Hat Hackers, Auditors Join Forces*, BLOCKWORKS (Aug. 8, 2023, 6:18 AM), <https://blockworks.co/news/defi-seal-911-white-hat-hackers-auditors>; Kelsie Nabben & Primavera De Filippi, *SEAL Drills: Attack Simulations to Improve Web3 Security* (Oct. 23, 2023), <https://kelsienabben.substack.com/p/the-chaos-team-attack-simulations>.

Andrea Gacki  
January 22, 2024  
Page 3

harm crypto users and projects—including those backed by Paradigm—and cast a pall over the entire crypto industry.

While FinCEN’s concerns about the potential abuse of these technologies are legitimate, the Proposed Rule misses the mark as to the source of the risk and the appropriate subject for regulation. Instead of focusing on the risk posed by bad actors that are laundering ill-gotten gains, the Proposed Rule identifies a broad class of technologies and activities as the source of this risk. By focusing on general technologies and activities with many applications, the Proposed Rule departs from FinCEN’s historical use of its authority under Section 311 of the Patriot Act, which has exclusively and effectively focused on a specific person, entity, or jurisdiction.

“CVC mixing” as defined by the Proposed Rule is the “facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used.”<sup>5</sup> This definition is overly broad and stands to impose enhanced reporting requirements on a broad swath of legitimate activities, many completely unrelated to what is commonly understood to be virtual currency mixing and used for legitimate purposes which do not present the same money laundering risk. Yet by suggesting that any technology or business model that has the effect of anonymizing the source, destination, or amount of a transaction is “of primary money laundering concern,” the Proposed Rule stigmatizes an array of important and useful technologies and would amount to yet another inapt federal government action that risks pushing legitimate crypto users and innovators away from the United States.

Numerous blockchain business models protect the privacy of blockchain transactions by anonymizing transaction data. Virtual currency mixers are but one example. While certain mixers have been abused by illicit actors who are themselves legitimate targets for regulatory action, mixers and related technologies are used by many law-abiding U.S. citizens for legitimate reasons. Blockchain transactions are publicly viewable. While wallet addresses are pseudonymous, if the owner of a wallet address is identified, they risk having all their transactions, including sensitive ones, exposed to the public and adverse actors. For example, a person wishing to donate crypto to Ukraine’s fundraising efforts to combat the Russian invasion has a legitimate interest in using a privacy enhancing technology to prevent Russia from tracking that crypto donation and potentially retaliating against them or their family. The legitimate interest in conducting private crypto transactions extends to the more commonplace example of an employee of an

---

<sup>5</sup> See Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72,701, 72,722 (proposed Oct. 23, 2023) (to be codified at 31 C.F.R. pt. 1010).

Andrea Gacki  
January 22, 2024  
Page 4

American company who is compensated in crypto and wishes to preserve some privacy over how they choose to spend their earnings, including donations to religious or political organizations.

Beyond privacy, innovators are exploring new solutions and technologies to drive down the cost and increase the speed of crypto transactions, which in some instances have the effect of anonymizing the source, destination or amount of virtual currency transactions, but do not raise the same money laundering concerns as virtual currency mixing. For instance, tools and technologies that bundle and process transactions off-chain to increase the speed and reduce the cost of transactions may have the effect of anonymizing the source, destination, or amount of a transaction.<sup>6</sup>

In finding “CVC mixing,” as defined by the Proposed Rule, to be of primary money laundering concern, the Proposed Rule stands to stigmatize numerous legitimate activities and significantly increase compliance costs for regulated financial institutions. A more targeted and nuanced approach is required—one that focuses on bad actors as the source of financial crime risk—not a vaguely defined class of business models and technologies. In this way, FinCEN can best balance the government’s interest in detecting and preventing financial crime with the community’s interest in sensible regulation that promotes legitimate uses of blockchain and distributed ledger technologies.

**III. The definitions of “CVC mixers” and “CVC mixing” are overly broad and, as written, will encompass numerous legitimate businesses, business models, technologies, and technology use cases.**

The Proposed Rule defines “CVC mixer” as “any person, group, service, code, tool, or function that facilitates CVC mixing” and, as mentioned above, “CVC mixing” as “the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used.”<sup>7</sup> By FinCEN’s own admission, these definitions are “broad.”<sup>8</sup> Indeed, they are overly broad.

These definitions would cover technologies far beyond what are commonly understood to be virtual currency mixers, such as Blender.io and Tornado Cash, or

---

<sup>6</sup> See Chainlink, What is a Layer 2? (May 24, 2023), <https://chain.link/education-hub/what-is-layer-2>.

<sup>7</sup> Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. at 72,722.

<sup>8</sup> See *id.* at 72,709 (“FinCEN acknowledges this definition is relatively broad.”).

Andrea Gacki  
January 22, 2024  
Page 5

their use, which is commonly understood to be virtual currency mixing. Instead of a narrow focus on specific services that have become implicated in use by malign actors, the definitions of “CVC mixer” and “CVC mixing” implicate many legitimate and innocuous blockchain-related technologies designed to increase the speed and scalability of blockchain activity, reduce transaction costs, and facilitate user privacy.

The six examples provided by FinCEN in the definition of “CVC mixing”<sup>9</sup> demonstrate the extraordinary breadth of the Proposed Rule. These six examples cover many activities, products, and services that are completely unrelated to virtual currency mixing and do not raise inherent money laundering and terrorist financing risks. Requiring financial institutions to report on transactions involving these activities goes well beyond the stated purpose of the Proposed Rule, which is to increase reporting related to virtual currency mixers, and would, in effect, create a generalized reporting requirement related to a huge swath of virtual currency activities, creating burdensome reporting obligations for financial institutions, and stifling legitimate activities. Furthermore, the sheer frequency and volume of transactions that would be captured would create an enormous burden for FinCEN to process and analyze. As we assume FinCEN’s intent in drafting the Proposed Rule was not to designate all or even a significant portion of crypto activities as a “primary money laundering concern,” these provisions need revision. We provide a selection of legitimate crypto development activities below that would be inappropriately targeted by this action.

- Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts. This general example could potentially capture activities that have nothing to do with virtual currency mixing but relate to basic trading activity that does not present inherent money laundering risks. For example, decentralized exchanges (“DEXs”) using automated market maker mechanisms (“AMMs”) rely on liquidity pools that aggregate digital assets from multiple persons in order to create a market between a certain trading pair. Therefore, a person that transfers assets from a regulated financial institution and deposits them in a liquidity pool with the intent to earn some return could be subject to the Proposed Rule’s reporting requirements.
- Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction. There are many rapidly developing crypto technologies that manage the structure of crypto transactions for legitimate applications. For example, DEX aggregators allow users that want to execute a trade between crypto assets to source liquidity between different

---

<sup>9</sup> *Id.* at 72,722.

Andrea Gacki  
January 22, 2024  
Page 6

exchanges. By splitting up a single trade across multiple DEXs, the DEX aggregator can reduce slippage and improve the user's trade execution. In addition, Paradigm and our partners in the crypto ecosystem have developed time-weighted average market makers ("TWAMMs"), which are a type of DEX that helps traders on Ethereum efficiently execute large orders by breaking long-term orders into many infinitely small pieces and executing them against an embedded constant-product AMM smoothly over time.<sup>10</sup> Both DEX aggregators and TWAMMs could fall within the definition of "CVC mixing," even though they do not present the risks intended to be addressed by the Proposed Rule. Additionally, new trading venues and blockchain protocols that rely on "intents"—where a user expresses a desired outcome for their transaction (e.g., best sale price for an asset) rather than an explicit command (e.g., trade X asset for Y asset at Z price), and the protocol determines the best way to achieve that outcome—could also be captured by this provision.<sup>11</sup>

- Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions. There are many legitimate applications of crypto technologies that split transactions into series of independent transactions which do not raise the money laundering or terrorism finance risks intended to be addressed by the Proposed Rule. In addition to DEX aggregators and TWAMMs discussed in the example above, which can also execute sequential buy orders over a period of time (known as "dollar cost averaging"), many "Layer 2" protocols that aim to increase the scalability of blockchains like Bitcoin or Ethereum could fall within FinCEN's proposed definition of "CVC mixing." These Layer 2 protocols attempt to increase the transaction throughput and lower the transaction cost of blockchains like Bitcoin or Ethereum, including in some instances by splitting transactions into a series of independent transactions. The potential application of the Proposed Rule to these types of Layer 2 protocols will have a sweeping impact on the crypto industry and would undermine ongoing efforts to speed the processing and reduce the cost of virtual currency transactions.
- Creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions. Use of a cold storage hardware device—a common

---

<sup>10</sup> See Dave White, Dan Robinson & Hayden Adams, *TWAMM*, PARADIGM (July 28, 2021), <https://www.paradigm.xyz/2021/07/twamm>.

<sup>11</sup> See Sam Kessler, *Intents Are Blockchain's New Buzzword. What Are They and What Are the Risks?*, COINDESK (Nov. 15, 2023), <https://www.coindesk.com/tech/2023/11/15/intents-are-blockchains-big-new-buzzword-what-are-they-and-what-are-the-risks/>.

Andrea Gacki  
January 22, 2024  
Page 7

security measure to guard against virtual currency theft—could fall within the definition of “CVC mixing,” if the cold storage hardware device is considered a single-use wallet, address, or account. Creating reporting requirements around cold storage devices would create a significant compliance challenge for financial institutions, who would have to determine whether a transaction involves a cold storage device, and could undermine the privacy and security of individuals seeking to use such devices. Further, there is no clarity around what time frame might constitute “single-use” for a wallet—as a wallet may be created, used once, and a financial institution consider it “single-use,” only for the wallet to be used again later in the normal course of user activity.

- Exchanging between types of CVC or other digital assets. As written, this example could implicate all ordinary-course transactions of digital assets on exchanges or decentralized finance platforms, which is an unreasonably broad target for reporting requirements. In addition, there are rapidly developing technologies that facilitate the interoperability of different blockchains by allowing users to “bridge” assets across. These bridging transactions would also be potentially subject to the reporting requirements even though they do not implicate the money laundering and terrorism finance risks FinCEN should be focused on.
- Facilitating user-initiated delays in transactional activity. Some DEX aggregators allow users to place delayed orders, which could fall within the definition of “CVC mixing,” as facilitation of a user-initiated delay in transactional activity. Such delayed orders would not appear to raise any additional money laundering or terrorist financing risks beyond ordinary virtual currency trading, and requiring financial institutions to report any transactions involving services that allow users to place delayed orders would further expand the scope and compliance burden related to the Proposed Rule. Further, as there is no definition of what constitutes a “delay,” services that order transactions for users within blocks themselves—providing maximally efficient execution—could fall within the scope of this provision.

Any one of the real-world examples described above could fall into the Proposed Rule’s definition of “CVC mixing.” When in doubt, financial institutions will almost certainly err on the side of caution rather than risking a possible violation of the Proposed Rule. Given the breadth and significant ambiguity of the definition of “CVC mixing,” financial institutions will either be forced to institute enhanced reporting over substantially all of their virtual currency transactions, or to de-risk such transactions. This is the definition of an unnecessary and unintentional chilling effect on the entire space.



Andrea Gacki  
January 22, 2024  
Page 8

**IV. The best tools to address concerns around CVC mixing are increased industry guidance and, where required to address specific bad acts, designations of specific bad actors under Section 311.**

The Proposed Rule, as structured, would create a de facto parallel SAR reporting regime, but one lacking in any meaningful assessment of financial crime risk and transaction-specific characteristics. To the extent that FinCEN is concerned about receiving SAR reporting on suspicious use of virtual currency mixing activities, as at least a first step it would be more appropriate to provide guidance to regulated financial institutions on its expectations as to SAR filing and virtual currency-related transactions. This would be consistent with the risk-based anti-money laundering regime in the United States and is likely to provide FinCEN and U.S. law enforcement authorities with the most relevant and actionable information about potential money laundering or terrorist financing activity. For example, FinCEN could offer guidance on expectations regarding use of blockchain analytics to assess whether what is commonly understood to constitute a virtual currency mixer has been used with respect to certain digital tokens or wallet addresses and regarding when a U.S. financial institution would be expected to file a SAR with respect to such blockchain analytics findings. Unlike the Proposed Rule, which would impose a significant reporting requirement regarding a broad swath of businesses, business models, technologies, and technology use cases—many of which do not raise any particular money laundering or terrorist financing risks—and would inundate FinCEN with information that may not be helpful for law enforcement purposes, guidance for U.S. financial institutions could help improve SAR quality and increase SAR reporting.

Paradigm also notes that, to date, FinCEN has reserved its Section 311 designations for specific actors that have been identified as having facilitated illicit activities. The U.S. Department of the Treasury has not hesitated to use its authorities to take action against services that raise money laundering and terrorist financing risks, including the designations of Blender.io and Tornado Cash by the Office of Foreign Assets Control. Focusing on specific malign actors, rather than targeting broad swaths of the crypto industry as under the Proposed Rule, would avoid the unintended consequences of the Proposed Rule and preserve America's competitive advantage in the digital assets space.

**V. Recommendations**

*FinCEN should work with industry to identify the highest risk activities associated with virtual currency mixers and issue SAR reporting guidance to address these risks.* The Proposed Rule suggests that imposing recordkeeping and reporting requirements under the Section 311 authorities would guard against

Andrea Gacki  
January 22, 2024  
Page 9

international money laundering and other financial crimes by increasing transparency in these transactions, rendering them less attractive to illicit actors, and providing additional information to support law enforcement investigations.<sup>12</sup> These same goals can be achieved by FinCEN providing guidance to clarify when companies should submit SARs involving potentially illicit activities. SARs are the appropriate vehicle for reporting concerning transactions and allow for financial institutions to assess risk and suspicion on the basis of an array of inputs. In consultation with industry, FinCEN should work to identify the highest risk activities associated with virtual currency mixers. The scope of these activities should be significantly narrower than those encompassed by the current definition of CVC mixing activities in the Proposed Rule. FinCEN should then issue guidance on the appropriate criteria to assess illicit activity, such as thresholds of activity, which can drive the collection of useful reporting without overly burdening financial institutions or flooding FinCEN with useless information. In this way, FinCEN can achieve the twin goals of collecting useful information on potential illicit activities and discouraging bad actors from exploiting these technologies.

***FinCEN should focus its Section 311 authorities on bad actors.*** FinCEN should focus the use of Section 311 actions to target, if necessary, specific virtual currency mixing services determined to have knowingly or recklessly facilitated illicit transactions. For instance, in February 2023, FinCEN identified the virtual currency exchange Bitzlato Limited as an entity of primary money laundering concern in connection with Russian illicit finance, an action coordinated with U.S. law enforcement and foreign partners.<sup>13</sup> FinCEN can similarly use its Section 311 authorities to identify and target other bad actors exploiting virtual currency mixers and other legitimate blockchain services and technologies.

***The definitions of “CVC mixing” and “CVC mixer” should be narrowed.*** While we believe that there are better ways of addressing the risk posed by bad actors exploiting virtual currency mixers, to the extent that FinCEN decides to pursue this Proposed Rule, the definition of “CVC mixing” would need to be revised to be objective, actionable, and narrowly focused. The definition should distinguish between services and activities commonly understood to be virtual currency mixing and other virtual currency services and activities that do not raise the same concerns.

---

<sup>12</sup> Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. at 72,707.

<sup>13</sup> See FinCEN, Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitlato, RIN 1506-AB42 (Feb. 1, 2023), [https://www.fincen.gov/sites/default/files/shared/Order\\_Bitzlato\\_FINAL%20508.pdf](https://www.fincen.gov/sites/default/files/shared/Order_Bitzlato_FINAL%20508.pdf).

Andrea Gacki  
January 22, 2024  
Page 10


***Engagement with the crypto industry is the best path forward.*** We are an American company and support U.S. efforts to address illicit finance. Rather than finalize this rule as proposed, we believe the best path forward for FinCEN, crypto, and the American people is FinCEN working with the crypto industry on solutions that actually reduce illicit activity and do not unfairly punish good actors or create unnecessarily burdensome reporting requirements on U.S. financial institutions. Many of FinCEN's best efforts on crypto have involved engagement with tech and financial firms through the exchange of information and ideas. The same well-trod path should be true when it comes to illicit activity and mixers.

\* \* \* \*

Again, we thank FinCEN for the opportunity to comment on this matter. We would be happy to discuss any of these issues with FinCEN staff. If you have any questions or comments, please feel free to contact us [rodrigo@paradigm.xyz](mailto:rodrigo@paradigm.xyz) or [agrieve@paradigm.xyz](mailto:agrieve@paradigm.xyz).

Sincerely,

DocuSigned by:  
  
D0AAB33798764AD...  
Rodrigo Seira,  
Special Counsel, Paradigm

DocuSigned by:  
  
EB96B2A10CD1491...  
Alex Grieve,  
Government Affairs Lead, Paradigm