

Andrea Gacki  
Director  
Financial Crimes Enforcement Network  
U.S. Department of the Treasury  
P.O. Box 39  
Vienna, VA 22183

January 22, 2024

**SUBMITTED ELECTRONICALLY**

**Re: *Docket Number FINCEN-2023-0016* – Proposal of Special Measure Regarding Convertible Virtual Currency Mixing as a Class of Transactions of Primary Money Laundering Concern**

Dear Director Gacki:

We appreciate the opportunity to comment on Docket Number FINCEN-2023-0016 (the “Mixing Transaction NPRM”), released by the Financial Crimes Enforcement Network (“FinCEN”) on October 22, 2023.<sup>1</sup> We are a variety of unaffiliated companies that rely on important cybersecurity safeguards and privacy-enabling software to protect our businesses and our users. The extreme breadth of the rules proposed by the Mixing Transaction NPRM would overly burden our use of such technologies in ways that would not assist FinCEN in achieving its mandate of preventing money laundering and other illicit use of money. As a result, we write to express our grave concerns regarding the novelty and scope of the Proposed Special Measures and the inadequate definitions contained therein.<sup>2</sup>

The Proposed Special Measures would unreasonably infringe upon the legitimate financial privacy interests of cryptocurrency users, and would apply to a variety of digital techniques that are not mixing transactions at all, but rather simply represent good cybersecurity practices. Moreover, the Proposed Special Measures are unnecessary to achieve FinCEN’s aim, and we encourage FinCEN to either withdraw the Mixing Transaction NPRM altogether or to pursue a less invasive, less restrictive, and more effective approach—the same approach it has used since its first enforcement activities in the cryptocurrency space in 2013—to enforcement against specific bad actors.

- 1. FinCEN should exercise caution and either withdraw entirely or narrowly tailor the Mixing Transaction NPRM because if adopted, the Mixing Transaction NPRM would not only represent the first time FinCEN used its Section 311 powers against a class of transactions, but also the first time FinCEN has ever imposed Special Measure 1.**

Historically, FinCEN has exercised caution in making designations under Section 311 and implementing Special Measures. Section 311 (31 U.S.C. 5318A), authorizes the U.S. Department

---

<sup>1</sup> FinCEN, Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, Dkt. FINCEN-2023-0016 (Oct. 22, 2023) [https://www.fincen.gov/sites/default/files/federal\\_register\\_notices/2023-10-19/FinCEN\\_311MixingNPRM\\_FINAL.pdf](https://www.fincen.gov/sites/default/files/federal_register_notices/2023-10-19/FinCEN_311MixingNPRM_FINAL.pdf) [hereinafter Mixing Transaction NPRM].

<sup>2</sup> In this regard, we intend this letter to specifically respond to FinCEN’s request for comments A(1)-(8), B(2)-(3), C(1), D(2), and D(11) as listed in the Mixing Transaction NPRM.

of Treasury (“Treasury”) to designate a foreign jurisdiction, financial institution, class of transactions, or type of account as being of “primary money laundering concern” and impose one or more of five possible “special measures.” Treasury delegated that authority to FinCEN, which has used its power quite sparingly since Section 311’s enactment. The first Section 311 action instituted by FinCEN in the virtual currency space occurred in 2013, when FinCEN instituted special measures against Liberty Reserve. Prior to that time, between 2002 and 2013, FinCEN had only ever implemented special measures against just four jurisdictions and 13 financial institutions. After a protracted legal battle regarding a Section 311 action between 2015-2017, FinCEN seemed reluctant to use its Section 311 powers widely.<sup>3</sup> The creation of the Global Investigations Division (GID) in 2019<sup>4</sup> and the enactment of the Anti-Money Laundering Act of 2020, which increased FinCEN’s authority “to prohibit or impose conditions upon certain transmittals of funds (to be defined by the Secretary) by any domestic financial institution or domestic financial agency,”<sup>5</sup> coincided with an uptick in the use of Section 311 powers and a broadening of FinCEN’s attention to all 5 available Special Measures.

Importantly, throughout its use of Section 311, FinCEN traditionally imposes Special Measure Number 5 to isolate a specific foreign financial institution and prevent it from accessing the U.S. financial system. Until this Mixing Transaction NPRM, FinCEN has only used Special Measure Number 1 one other time—in 2012 against JSC CredexBank (“Credex”).<sup>6</sup> FinCEN later withdrew that proposed rule in 2016.<sup>7</sup> If adopted, the Mixing Transaction NPRM would constitute the first time FinCEN has imposed Special Measure Number 1 in exercising its Section 311 Powers. Moreover, this Mixing Transaction NPRM represents the very first time FinCEN has sought to designate an entire class of transactions as a primary money laundering concern. We encourage FinCEN to exercise extreme caution in the exercise of its Section 311 powers in such a novel way—the first-ever designation of a class of transactions and the first-ever imposition of Special Measure 1.

Exercising caution in Section 311 powers reflects the seriousness of Treasury’s policy purposes for invoking its powers to make primary money laundering concern designations and impose special measures—namely, to act as a signal to the world that FinCEN is “serious about ensuring that the international financial system is safeguarded against the threat of money laundering.”<sup>8</sup> As Treasury explained in the press release announcing the very first use of its Section 311 powers in 2002, when FinCEN uses Section 311, “[FinCEN] tell[s] the world clearly that these jurisdictions [or entities or transactions] are bad for business and that their financial controls

---

<sup>3</sup> See *FBME Bank Ltd. v. Lew*, 125 F. Supp. 3d 109 (D.D.C. 2015); *FBME Bank Ltd. v. Lew*, 142 F.Supp.3d 70 (D.D.C. 2015); *FBME Bank Ltd. v. Lew*, 209 F.Supp.3d 299 (D.D.C. 2016); *FBME Bank Ltd. v. Munchin*, 249 F. Supp.3d 215 (D.D.C. 2017).

<sup>4</sup> FinCEN, Press Release, *New FinCEN Division Focuses on Identifying Primary Foreign Money Laundering Threats* (Aug. 28, 2019),

<https://www.fincen.gov/news/news-releases/new-fincen-division-focuses-identifying-primary-foreign-money-laundering-threats>. We note with some alarm that the timing of GID’s creation coincided with the release of FinCEN’s 2019 CVC guidance, indicating that perhaps the two were coordinated and greater targeting of CVC users has been underway for some time.

<sup>5</sup> 2021 NDAA, Section 9714, <https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf>.

<sup>6</sup> 77 Fed. Reg. 31,794 (Mar. 30, 2012).

<sup>7</sup> 81 Fed. Reg. 14,408 (Mar. 17, 2016).

<sup>8</sup> U.S. Dept. Treas., Press Release, *Fact Sheet Regarding the Treasury Department’s Use of Sanctions: Authorized Under Section 311 of the USA PATRIOT ACT* (Dec. 20, 2002), <https://home.treasury.gov/news/press-releases/po3711>.

cannot be trusted.”<sup>9</sup> For the reasons further explained below, FinCEN’s targeting of convertible virtual currency (“CVC”)<sup>10</sup> purported “mixing” transactions does not achieve these aims. Rather than target transactions that are “bad for business,” the Mixing Transaction NPRM targets an overly broad range of technical approaches used as best practices both by businesses and individuals for ensuring the security of CVC and impinges on privacy rights of legitimate users of CVC. In an attempt to exercise authority it has never used before (class of transactions) through a special measure it has never previously imposed successfully (special measure 1), FinCEN created a proposed rule fraught with misunderstandings and overreach. We urge FinCEN to withdraw the rule and reconsider its approach to this novel use of its authority.

**2. The Mixing Transaction NPRM proposes a rule that is an improper and overbroad application of Section 311 measures to achieve transaction surveillance and suppression that FinCEN does not otherwise have a lawful basis to undertake.**

Although the Mixing Transaction NPRM ostensibly designates a class of transactions as being of Primary Money Laundering Concern, its real goal is to uncover an alternative method for collecting information about and suppressing the use of digital currency in general. The Mixing Transaction NPRM is an improper and overbroad application of Section 311 measures for that purpose. Indeed, although the Mixing Transaction NPRM allegedly sanctions a class of transactions, it inconsistently throughout refers to “CVC mixers,” “CVC mixing” and “CVC mixing services” by reference to specific business entities<sup>11</sup> and as a type of business model more generally.<sup>12</sup> If FinCEN has reason to believe specific entities conduct illicit activities, FinCEN could use the Section 311 powers it has traditionally and successfully used to target specific entities as financial institutions of primary money laundering concern. Such an approach offers a more targeted way to address actual money laundering while protecting legitimate users of legitimate privacy-enhancing tools.

Notably, Treasury has separately sanctioned what it refers to as CVC mixing transactions through its Office of Foreign Asset Control (OFAC) authority to designate people or property who conduct transactions with specifically designated foreign jurisdictions identified through executive order as posing terrorist threats.<sup>13</sup> Treasury is currently facing legal challenges to, and has been widely criticized for, its attempt to sanction the Tornado Cash open source software as property of a non-existent entity Treasury alleges is called “the Tornado Cash DAO entity.”<sup>14</sup>

---

<sup>9</sup> *Id.*

<sup>10</sup> We note that we dislike the term convertible virtual currency, as it does not fit industry understanding of the technical realities of cryptocurrencies and their many uses. We use the term in this letter only because it is the language that FinCEN has adopted for the implementation of its regulations. As an aside, we would encourage FinCEN to adopt more technically accurate vocabulary for implementing its regulations, as doing so would help FinCEN avoid proposing unworkable and overbroad regulations such as the Mixing Transaction NPRM.

<sup>11</sup> *See, e.g.*, Mixing Transaction NPRM, *supra* note 1, at 15 (“ChipMixer, a darknet CVC ‘mixing’ service”); 16 (referring to Bestmixer.io as a CVC mixing transaction); 20 (referring to enforcement against “Bitcoin Fog”).

<sup>12</sup> *See, e.g., id.* at 5 (“persons who facilitate...CVC mixing transactions”); 18 (“RAILGUN falls under the umbrella of CVC mixing...because it uses its privacy protocol to manipulate the structure of the transaction to appear as being sent from the RAILGUN contract address, thus obscuring the true originator.”); 20 (“CVC mixing services often deliberately operate opaquely...”.)

<sup>13</sup> U.S. Dpt. Treas., Press Release, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), <https://home.treasury.gov/news/press-releases/jy0916>.

<sup>14</sup> *See, e.g., Van Loon et. al., v. OFAC*, No. 23-506669 (5th Cir. 2023) (notably, a variety of amici intervened with arguments critiquing the OFAC sanction at both the District Court and 5<sup>th</sup> Circuit Court of Appeals); Peter Van

Although we agree with the many arguments as to why Treasury’s OFAC action with regard to Tornado Cash software is an example of agency overreach, we wish to make a different but related point here. To justify its OFAC sanctions against the Tornado Cash software, Treasury had to designate the software as property of an entity.<sup>15</sup> OFAC officially explained as part of defending its sanction to a judge that the Tornado Cash software was property under Treasury’s regulations because it fell within the broad reach of “any contract whatsoever.”<sup>16</sup> Although the definition of “transaction” under the BSA regulations is quite broad, it does not encompass “any contract whatsoever” but rather centers on monetary transfers and specific services offered by financial institutions, and provides a catch-all for “any other payment, transfer, or delivery by, through or to a financial institution, by whatever means effected.”<sup>17</sup> No part of the definition applicable to CVC mixing is also a contract.<sup>18</sup>

In other words, in proposing the Mixing Transaction NPRM, one arm of Treasury is classifying CVC mixing as a transaction type while another arm of Treasury argues that mixing is a contract for services. Under the regulations governing both enforcement actions, mixing activity cannot be both a transaction type and a contract for service simultaneously. Treasury’s attempt to designate mixing software as both a type of transaction and a contract is evidence of the arbitrary and capricious nature of its attempt to regulate open-source software that enhances the digital privacy of legitimate CVC users. To the extent that FinCEN really wants to target non-custodial, open-source software that individuals can use on their own accounts, FinCEN exceeds its statutory authority.

Indeed, tools that enhance digital privacy in CVC transactions simply seek to enable a form of digital cash. As a result, in its rush to find a way to suppress CVC mixing transactions, by whichever means, even if inconsistent amongst different internal branches of its own agency, FinCEN’s Mixing Transaction NPRM amounts to an attempt to sanction “all transactions conducted in cash,” which is both impossible and an unreasonable over-extension of its rulemaking authority.

### **3. The Mixing Transaction NPRM should be withdrawn because the proposed definition of “CVC mixing” is overbroad and targets lawful activity in a way that makes the agency’s proposed action arbitrary and capricious.**

---

Valkenburgh, *New Tornado Cash Indictments Seem to Run Counter to FinCEN Guidance*, COINCENTER (Aug. 23, 2023), <https://www.coincenter.org/new-tornado-cash-indictments-seem-to-run-counter-to-fincen-guidance/>.

<sup>15</sup> OFAC, FAQ 1095, <https://ofac.treasury.gov/faqs/1095> (“OFAC designated the entity known as Tornado Cash, which is a “partnership, association, joint venture, corporation, group, subgroup, or other organization” that may be designated pursuant to the IEEPA.”).

<sup>16</sup> See, Order, *Van Loon et. al. v. Dpt. Treas.*, 1:23-CV-312-RP at 18 (W.D. Tx. Aug. 17, 2023).

<sup>17</sup> 31 CFR 1010.100(bbb)(1). “Except as provided in paragraph (bbb)(2) of this section, transaction means a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, security, contract of sale of a commodity for future delivery, option on any contract of sale of a commodity for future delivery, option on a commodity, purchase or redemption of any money order, payment or order for any money remittance or transfer, purchase or redemption of casino chips or tokens, or other gaming instruments or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected.”

<sup>18</sup> Notably, in the Mixing Transaction NPRM, FinCEN refers to Tornado Cash as a “CVC mixer,” not as a CVC mixing transaction. Is mixing a transaction? Is mixing a contract? Is mixing a type of business? The fact that FinCEN cannot decide belies the inappropriateness of using its Section 311 sanctions as proposed.

Setting aside FinCEN’s own apparent confusion about whether CVC mixing is a transaction, a service, a business, or a specific business entity, when FinCEN does attempt to define the “class” of transactions that it considers to be CVC mixing, the Mixing Transaction NPRM’s definition of “mixing” is extremely broad and includes numerous activities routinely conducted by legitimate users as a matter of routine safety precautions in online transacting in CVC. Specifically, the Mixing Transaction NPRM provides:

The term “CVC mixing” means 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, such as: (1) pooling or aggregating CVC from multiple persons, wallets, addresses or accounts; (2) using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction; (3) splitting CVC for transmittal and transmitting the CVC through a series of independent transactions; (4) creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions; (5) exchanging between types of CVC or other digital assets;<sup>19</sup> or (6) facilitating user-initiated delays in transactional activity.<sup>20</sup>

Indeed, most of the activities captured by the proposed definition of CVC mixing are considered established best practices within the industry for the use and safekeeping of CVC. Specifically, the proposed definition encompasses lightning transactions, single-use wallets, atomic swaps, decentralized finance protocols, privacy coin features, and multi-signature wallets, among other things. The main commonality among this broad range of software tools is that they enhance digital privacy and offer basic cyber-security techniques to owners or custodians of CVC. Employing these techniques to safeguard valuable digital assets is as routine and mundane and free of illicit purpose as using two-factor authentication to secure a digital wallet containing payment card information or an X (formerly Twitter) account to prevent an unauthorized announcement.<sup>21</sup>

**4. The Mixing Transaction NPRM should be withdrawn because its inaccurate depiction of standard security practices as “mixing” impermissibly restricts the capacity of users to protect their property so that FinCEN can conduct a fishing expedition.**

---

<sup>19</sup> We note that the Mixing Transaction NPRM does not include a definition of “other digital assets” anywhere. Further, we are unaware of any definition of “digital assets” in FinCEN’s regulations or guidance. Finally, it is not clear to us how FinCEN has authority to impose regulatory reporting requirements upon exchanges of CVC for digital assets that are not CVC. See FinCEN, *Application of FinCEN’s Regulations to Persons Administering, Exchanging or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013) (the phrase “digital assets” appears nowhere in the 2013 Guidance); FinCEN, *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019) (the only time that the phrase “digital assets” appears in the 2019 Guidance is in footnote 75 in reference to the title of the SEC “Framework for Investment Contract Analysis of Digital Assets”). This is just another small but notable way in which FinCEN seeks to overreach its authority through the Mixing Transaction NPRM.

<sup>20</sup> Mixing Transaction NPRM, *supra* note 1, at 30-31.

<sup>21</sup> True Tamplin, *How to Protect Your Digital Wallet from Cyber Threats*, FORBES (Dec. 19, 2023, 2:00 pm EST), <https://www.forbes.com/sites/truetamplin/2023/12/19/how-to-protect-your-digital-wallet-from-cyber-threats/?sh=1e9146825981> (noting the importance of 2FA for securing digital wallets).

The proposed rule describes as red flags such everyday practices as “creating and using single address wallets” and “splitting CVC for transmittal.”<sup>22</sup> The standard practice among cryptocurrency users is to change addresses with every transaction. For example, Coinbase Exchange describes to their users that: “[w]e automatically generate a new address for you after every transaction you make or when funds are moved between your wallet and our storage system. This is done to protect your privacy, so a third party cannot view all other transactions associated with your account simply by using a blockchain explorer.”<sup>23</sup>

The fact that a small subset of users, who may be criminals, engage in the same operational security practices as ordinary users does not make those operational security practices suspect. The fact that criminals may use two-factor authentication to protect the security of their online applications does not mean that the use of two-factor authentication is itself an indicator or facilitator of criminal activity. In exactly the same way, the fact that users do not reuse Bitcoin addresses is merely indicative of basic operational security.

In an apparent recognition of the fact that these tools legitimately enable important cyber-security precautions, FinCEN exempts financial institutions from reporting on any of their own mixing transactions that they may conduct in the course of providing services to the public.<sup>24</sup> By exempting financial institutions from the rule, FinCEN creates a regime where financial institutions can take proper cyber-security measures for using CVC, but regular people cannot.

Perhaps even more problematic, throughout the Mixing Transaction NPRM, FinCEN justifies the proposed rule as necessary to enable law enforcement and the agency to better understand the transactions and the extent to which illicit activity occurs through CVC mixing.<sup>25</sup> The extraordinary and never before successfully invoked Section 311 power to designate a class of transactions and implement special measure 1 is not appropriate for use in a fact-finding mission. Employing such overly broad definitions as proposed in the Mixing Transaction NPRM for the purpose of authorizing an invasive fact-finding mission represents an arbitrary and capricious use of FinCEN’s delegated rulemaking authority because FinCEN’s justification for the rule lies outside of the statutory criteria for determining a class of transactions is of primary money laundering concern.

Specifically, FinCEN is statutorily required to consider the following factors when determining that a class of transactions is of primary money laundering concern: (1) the extent to which the class of transactions is used to facilitate or promote money laundering in or through a jurisdiction outside of the United States, including money laundering activity with connections to international terrorism, organized crime, and proliferation of WMDs and missiles; (2) the extent to which a class of transactions is used for legitimate business purposes; and (3) the extent to which action by FinCEN would guard against international money laundering and other financial

---

<sup>22</sup> Mixing Transaction NPRM, *supra* note 1, at 30-31.

<sup>23</sup> See <https://help.coinbase.com/en/exchange/managing-my-account/crypto-address-change>

<sup>24</sup> Mixing Transaction NPRM, *supra* note 1, at 31.

<sup>25</sup> See, e.g., *id.* at 24 (“Furthermore, the information generated by this special measure would support investigations into illicit activities by actors who make use of CVC mixing to launder their ill-gotten CVC by law enforcement. At present, there is no similar or equivalent mechanism possessed by law enforcement to readily collect such information, depriving investigators of the information necessary to more effectively understand, investigate and hold illicit actors accountable.”).

crimes.”<sup>26</sup> Throughout the Mixing Transaction NPRM, FinCEN acknowledges that due to a lack of data and a lack of understanding of CVC mixers, it cannot sufficiently assess the extent to which CVC mixing and the proposed rule measures up under any of these three criteria.<sup>27</sup> FinCEN’s assessment ultimately boils down to: FinCEN does not have sufficient information to properly assess the statutory criteria required to justify the proposed rule, so the proposed rule is justified because, in FinCEN’s own words, it “is necessary to better understand the illicit finance risk posed by CVC mixing.”<sup>28</sup> Using a sanction to obtain the information necessary to justify imposing the sanction even when the agency knows that doing so will likely impose a high burden on legitimate uses and financial institutions is the definition of arbitrary and capricious regulatory action.

**5. The Mixing Transaction NPRM should be withdrawn or significantly narrowed in scope because FinCEN’s required statutory analysis fails to adequately value the legitimate uses of CVC mixing services and unduly burdens legitimate users and financial institutions.**

FinCEN admits that public blockchains “make it possible to know someone’s entire financial history on the blockchain”<sup>29</sup> and that it “recognizes that there are legitimate reasons why responsible actors might want to conduct financial transactions in a secure and private manner given the amount of information available on public blockchains.”<sup>30</sup> Yet, in the same document, alleges that the Mixing Transaction NPRM is necessary because CVC “is not without its risks and, in particular, the use of CVC to anonymize illicit activity undermines the legitimate and innovative uses of CVC.”<sup>31</sup> These two propositions cannot be simultaneously accurate.

As a matter of technical reality, FinCEN’s assertion that public blockchains expose a user’s entire financial history on the blockchain to the public for everyone to see and inspect is correct.<sup>32</sup> Indeed, that creates the fundamental need for legitimate CVC users to conduct CVC mixing transactions—to reintroduce the same level of financial privacy that they enjoy in the traditional financial system<sup>33</sup> to their transactions via CVC (for example, the traditional financial system does not expose a consumer’s entire credit card history to the public, and indeed, federal law requires that financial institutions protect such information from being exposed to the public<sup>34</sup>).<sup>35</sup>

---

<sup>26</sup> 31 U.S.C. 5318A(a)(1).

<sup>27</sup> See Mixing Transaction NPRM, *supra* note 1, at 19 (not enough data to know how much CVC mixing is used in money laundering); 22 (not enough “available transactional information” for FinCEN to “fully assess the extent to which or quantity thereof CVC mixing activity is attributed to legitimate purposes”); 22 (essentially claiming that FinCEN’s lack of information itself is reason enough to show that getting more information would guard against international money laundering).

<sup>28</sup> *Id.* at 23.

<sup>29</sup> *Id.* at 7.

<sup>30</sup> *Id.* at 21.

<sup>31</sup> *Id.* at 6-7.

<sup>32</sup> Matthias Nadler & Fabian Schar, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, 105 FED RES. BK. ST. LOUIS REV. 122 (2023); Vitalik Buterin, et. al., *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium* (Sept. 9, 2023) (unpublished manuscript), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4563364](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364)

<sup>33</sup> See, e.g., 12 U.S.C. §§ 3401-3423 (the Right to Financial Privacy Act of 1978 (RFPA), which protects the confidentiality of personal financial records by creating a statutory fourth amendment protection for bank accounts).

<sup>34</sup> 16 C.F.R. Part 314, 67 Fed. Reg. 36484 (May 23, 2002) (FTC rule addressing the requirement that covered financial institutions safeguard non-public information”)

<sup>35</sup> Matthias & Schar, *supra* note 32.

Ensuring their CVC transactions enjoy the same level of privacy as transactions in traditional finance reduces the potential danger of personal harm to legitimate users and enables legitimate users to avoid waiving their constitutional right to privacy. When the identity of a legitimate CVC user is known and connected to the wallets holding CVC assets, the user becomes a target for kidnap, robbery, extortion, and hacking schemes.<sup>36</sup> Further, because of this inherent transparency by design of public blockchains, the Fifth Circuit recently ruled that no expectation of privacy exists for users of permissionless public blockchains who take no additional action to privacy-protect their transactions.<sup>37</sup> Legitimate users employ privacy-enhancing software when transacting in CVC in order to avoid inadvertently waiving their constitutionally protected privacy rights.

Ultimately, FinCEN has completely failed in its obligation to adequately account for the impact on legitimate users as required by its rulemaking authority. In defending its selection of special measure 1 over 2 through 5, FinCEN emphasizes, without explanation, that special measure 1—additional record keeping—allows legitimate users to continue using privacy-enhancing software without interruption.<sup>38</sup> This is false, as covered entities must report on any transaction that may have involved CVC mixing and a foreign jurisdiction. Indeed, read broadly, it is possible that the rules proposed by the Mixing Transaction NPRM require reporting on transactions that involve CVC that were transacted through mixing software at any point in the asset’s transaction history. Such reporting directly impedes the reasons for which legitimate users employ mixing software (to enhance financial privacy) by requiring the elimination of financial privacy (it is not a private transaction if an intermediary must surveil and report on the transaction). Software tools like mixers that enhance digital financial privacy provide a true electronic equivalent to cash. Notably, transactions in cash are not subject to rules such as those proposed in the Mixing Transaction NPRM. In an apparent acknowledgment of this deep and inherent conflict between the rules proposed by the Mixing Transaction NPRM and the legitimate uses to which legitimate users put CVC mixing software, FinCEN itself predicts that the rule will chill the use of CVC mixers.

**6. The Mixing Transaction NPRM should be withdrawn because it requires covered financial institutions to perform law enforcement’s function to accomplish FinCEN’s AML goals, which FinCEN, DOJ, and law enforcement can achieve using existing tools when they have a proper legal basis to employ those tools.**

Like the definitions of CVC mixing and CVC mixer, the Mixing Transaction NPRM’s information reporting requirements demonstrate a deep lack of technological understanding. Notably, all of the transaction information that the Mixing Transaction NPRM proposes to include in required reports by covered financial institutions involves data that, in most circumstances, FinCEN can just as easily obtain itself through blockchain data analytics. Similarly, the customer information that FinCEN would require covered financial institutions to report includes the same kinds of information such institutions must already report if a

---

<sup>36</sup> For a documented timeline of physical attacks on Bitcoin users, see *Known Physical Bitcoin Attacks*, GitHub <https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md> (last visited Jan. 22, 2024).

<sup>37</sup> See *United States v. Gratoski*, No. 19-50492 (5th Cir. 2020).

<sup>38</sup> Mixing Transaction NPRM, *supra* note 1, at 25 (special measure 1 is the only special measure that will preserve “legitimate actors’ ability to continue conducting secure and private financial transactions.”).



transaction raises sufficient red flags to trigger the filing of a Suspicious Activity Report (SAR). Nevertheless, the Mixing Transaction NPRM seeks to require covered financial institutions to file such reports on every single transaction for which the CVC involved may have ever been transacted through the extremely broad set of software that FinCEN's proposed rule defines as CVC mixing software. In other words, because law enforcement investigations into activity involving CVC are sometimes more difficult, FinCEN seeks to impose broad surveillance of individuals without cause through covered financial institutions. Covered financial institutions should not have to become *de facto* law enforcement officers to make investigations easier for FinCEN.

FinCEN, the Department of Justice, and law enforcement have previously and successfully employed the very tools FinCEN asks financial institutions to use for reporting compliance under the Mixing Transaction NPRM to target specific illicit actors. FinCEN has demonstrated that it knows how to properly investigate and enforce against specific custodial CVC mixing service providers that are not complying with the regulations to which they are subject. Specifically targeting illicit actors about which FinCEN and law enforcement have built a clear, strong case using the available blockchain data analytics tools better balances the need to combat illicit CVC mixing with the legitimate use of CVC mixing by individuals seeking to protect their legitimate, constitutionally and statutorily protected privacy interests.

For all of the reasons discussed above, we urge FinCEN to withdraw the Mixing Transaction NPRM altogether.

Thank you for your consideration.

If you have any questions or would like additional information, please see the contact information below:

Rafael Yakobi, Esq.  
*Managing Partner*  
The Crypto Lawyers, PLLC.  
rafael@thecryptolawyers.com  
(619) 317-0722



**THE CRYPTO LAWYERS**

**Signatories Appear on Next Page**

Sincerely,



**SAMOURAI WALLET**



**RIVER**



**STRIKE**



**RoninDojo**



**Swan**



**primal**



**GRIID**

**zaprite**



**Peach**



**mempool  
.space**



**upstream DATA**



**stak**



**VOLTAGE**

**Coinkite**

**Mutiny**



**SATOSHI ENERGY**



**Cathedral**



**AnchorWatch**



**bitnob**



**OSHI**



**BATTERY**



**FOLD**

**START9**

[Samurai Wallet](#), [Ten31](#), [River](#), [Strike](#), [RoninDojo](#), [Swan Bitcoin](#), [Primal](#), [GRIID](#), [Zaprite](#), [Peach](#), [Mempool Space](#), [Upstream Data](#), [Stakwork](#), [Vida Global](#), [Voltage](#), [Coinkite](#), [Mutiny Wallet](#), [Standard Bitcoin Company](#), [Satoshi Energy](#), [Cathedral Bitcoin](#), [AnchorWatch](#), [Bitnob](#), [Oshi](#), [Battery Finance](#), [Fold](#), [Start9](#)