January 22, 2024

Via electronic submission: http://www.regulations.gov

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: FinCEN Docket No. FINCEN-2023-0016 (Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern)

To Whom it May Concern:

LeXpunK[1] appreciates the opportunity to provide feedback on FinCEN's Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern (the "**Proposal**"). As the world continues its shift towards an increasingly digital age, economic activities are following suit. Consequently, bad actors are showing a growing tendency to engage in cybercrime and not just in crypto. Government servers have been hacked, traditional banking institutions have been frequent victims of phishing, data breaches and exploits, and individual users have been exposed to an ever-increasing number of scams that take advantage of technological illiteracy and bad security practices.[2] While we understand the drivers for the Proposal, and share the concerns set forth in the press release for the Proposal,[3] the rulemaking to address these issues must be evenly applied, risk-based, and fit for purpose.

The current Proposal meets none of these criteria and instead seeks to vilify a particular technology rather than address the root cause transactions cited in the Proposal as involving "likely illicit sources."[4] The risks

[1] LeXpunK is a builder-centric community of lawyers and developers focused on advocacy for decentralized technology through a number of avenues, each pursued in parallel. LeXpunK directs its efforts at (i) formulating and advocating for the development of clear and well-tailored policies and regulation that advance best practices while protecting the values of openness, transparency, and decentralization; (ii) developing model legal standards and structures; and (iii) constructing best practices as well as crypto native solutions (self-help and self-regulatory practices). LeXpunK is founded on the belief that lawyers have both a role and duty to contribute to the open source movement as it is incumbent upon us all as members of builder-communities to be active in shaping narratives and advocating for smart policy outcomes.

[2] Though we could cite countless examples, for a sampling of the broader issue showing the range of actors impacted as well as the pace of cyber exploits, *see e.g.* Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions," available at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (providing a timeline encompassing approximately 200 cyber incidents involving financial institutions up to 2022). *See also* Center for Strategic & International Studies, "Significant Cyber Incidents," available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (maintaining a timeline resource documenting "significant cyber incidents since 2006," with a focus on cyberattacks targeting government agencies, defense and high-tech companies, or economic crimes resulting in losses exceeding one million dollars); Federal Trade Commission (FTC), June 8, 2023, "New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam," available at https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam (citing reported consumer losses totaling $330 attributed to text scams in 2022); U.S. Government Accountability Office (GAO), April 22, 2021, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," available at https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (underscoring the imperative need for the federal government to expeditiously enhance national cybersecurity efforts in light of serious and rapidly evolving threats, while also noting that ensuring the nation's cybersecurity has been a persistent concern listed on the High Risk List since 1997).

[3] *See* Press Release, FinCEN, October 19, 2023, "FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing" (hereinafter "**Proposal Press Release**"), available at https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.

[4] Proposal at 5.

posed by online bad actors in an increasingly online world are ubiquitous. Implying a false correlation between crime and the facilitation thereof by the development and use of permissionless technology is an attempt to paint every developer, business, and user of this technology with not just an air of suspicion, but an adverse influence under law – that the technology, its developers, and its users, are perpetrators of crime and illicit activity when it occurs, as opposed to victims.[5]

It also falsely suggests that new ways of obfuscating crime[6] are being developed in the permissionless technology space that need to be urgently addressed by this drastic and far-reaching rulemaking. This is decidedly not the case. Indeed, the Tornado Cash and subsequent regulatory actions against mixers[7] have already had, and will continue to have, a material chilling impact on privacy[8] and the development of privacy-preserving technology, particularly in the U.S.[9] In the short time since the Tornado Cash designation, we have observed (i) OFAC sanctions modifying developer[10] and user behavior, chilling the use of mixers; (ii) law enforcement efforts continue to effectively track on-chain transactions of criminals by leveraging the underlying technology that, by its nature, makes entire transaction histories public by default[11] and (ii) significant industry efforts to adapt to and address underlying regulatory concerns around mixers, such as the development of Privacy Pools[12] and Circle's Recoverable Wrapper Tokens.[13] These

[5] FinCEN pays lip service to the right to privacy in the Proposal while referencing CVC mixing transactions (as described in *infra* note 7) and acknowledges "CVC mixing may be used for legitimate purposes, such as privacy enhancement for those who live under repressive regimes or wish to conduct licit transactions anonymously". Yet FinCEN ignores the impact of regulatory designations and enforcement while now seeking to make practically all transactions on-chain reportable. While this is not the main focus of our comment, we find the villainization of privacy-preserving technology incredibly detrimental to the stated goal of advancing national security interests as (i) most immediately, privacy tech is essential for protecting U.S. interests abroad, including (funding) dissidents of authoritarian regimes and (ii) this would inevitably continue to push innovation offshore.

[6] *See infra* discussion in Section I(A).

[7] *See* Press Release, U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," August 8, 2022, https://home.treasury.gov/news/press-releases/jy0916; Press Release, U.S. Department of the Treasury, "Treasury Designates DPRK Weapons Representatives," November 8, 2022, https://home.treasury.gov/news/press-releases/jy1087 (announcing that "OFAC simultaneously delisted and redesignated Tornado Cash under E.O. 13722 and E.O. 13694, as amended, for its role in enabling malicious cyber activities, which ultimately support the DPRK's WMD program"); and Press Release, Department of Justice, "Tornado Cash Founders Charged with Money Laundering and Sanctions Violations," August 23, 2023, https://www.justice.gov/opa/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations (hereinafter collectively "**Tornado Cash Regulatory Actions**"); *see also* Press Release, "Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency," November 29, 2023, https://home.treasury.gov/news/press-releases/jy1933 (relating to Sinbad.io).

[8] If we look at on-chain data, Tornado Cash daily deposits peaked on March 28, 2022 at 2,210 before pulling back roughly 90% to 238 on August 15, 2022 and maintaining similarly depressed levels thereafter. *See* https://dune.com/hildobby/tornado-cash for underlying data. The broader impact has been described by CoinCenter as an attack on something that "is merely a software-based privacy tool and it only ever does what its users want it to do." By targeting " Americans' freedom to use [a] tool, even for legitimate privacy reasons" regulators are not only failing to weigh legitimate purposes for seeking anonymity against the harms but are seeking to put their thumb on the scale to create a presumption of illegality. See Coin Center, Tornado Cash is No Golem, It's a Tool for Privacy and Free Speech, https://www.coincenter.org/tornado-cash-is-no-golem-its-a-tool-for-privacy-and-free-speech/.

[9] In the wake of the Tornado Cash Regulatory Action, there have been attempts to satisfy regulatory concern while preserving a degree of privacy. One such experiment has been Privacy Pools, which "at a non-custodial, non-restrictive privacy protocol that allows withdrawals to positively associate with arbitrary subsets of deposits. Users can voluntarily remove themselves from an anonymity set containing stolen or laundered funds, and this is done completely in zero knowledge without sacrificing the privacy of the user. This design aims to be a crypto-native solution that allows the community to defend against hackers abusing the anonymity sets of honest users without requiring blanket regulation". See Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani, "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium" (September 6, 2023), available at https://ssrn.com/abstract=4563364. Documentation available at https://github.com/ameensol/privacy-pools (hereinafter "**Privacy Pools**").

[10] The last development activity for Tornado Cash consisted of code commits made in August 2022. Following the designation, GitHub initially banned the Tornado Cash repositories, only to later partially reinstate them in read-only mode following guidance from OFAC. See GitHub Unbans Tornado Cash Repositories Following OFAC Guidance, Cointelegraph (available at https://cointelegraph.com/news/github-unbans-tornado-cash-repositories-following-ofac-guidance); for a developer activity chart, refer to https://defillama.com/protocol/tornado-cash?devMetrics=false&groupBy=cumulative&devCommits=true&tvl=false. For additional information, see also GitHub Restores Tornado Cash's Code in Read-Only Mode, The Block (available at https://www.theblock.co/post/172339/github-restores-tornado-cashs-code-in-read-only-mode).

[11] As acknowledged in the Proposal on page 7, "[t]he public nature of most CVC blockchains, which provide a permanent, recorded history of all previous transactions, make it possible to know someone's entire financial history on the blockchain."

[12] *See supra* note 9.

[13] Circle, "A Configurable and Programmable Wrapper Mechanism for Recovering ERC-20 Tokens" (available at https://www.circle.com/blog/a-configurable-and-programmable-wrapper-mechanism-for-recovering-erc-20-tokens) (describing the use cases and a design to "protect developers and users from thefts and illicit finance").

efforts are in addition to the diverse and ongoing industry-coordinated efforts to detect vulnerabilities before bad actors are able to exploit them, increase security standards, and provide heightened and coordinated remedial measures in the face of hacks.

While we believe the impetus for the Proposal is fundamentally flawed, the current Proposal is also unprecedented in its approach, its breadth, its uneven application, and its overreach. For the first time, it identifies an entire class of transactions as being "of primary money laundering concern".[14] It defines a CVC mixer as "any person, group, *service, code, tool, or function* that facilitates CVC mixing".[15] It trades the underlying and important policy goal of addressing bad actors to attempting to impose insurmountable burdens on the use and adoption of permissionless technology - a very troubling trend from the perspective of civil liberties and what seems to be a continued effort by policymakers at vilifying technological innovation rather than leveraging its capabilities to aid the stated policy end goal. It also uses an anti-money laundering authority citing the need to address 'mixing' while drastically and simultaneously expanding the definition to cover a whole new host of behaviors – none of which constitute money laundering.[16] **For reasons that we describe further below, our worry is that the Proposal in its current form will be counterproductive to meeting the stated objectives, impose unprecedented burdens, be harmful to user safety, U.S. competition and interests while continuing to push technological innovation offshore**.

As indicated above, our concerns are far-reaching. We believe the Proposal positioning an entire class of transactions as being "of primary money laundering concern" is a breathtaking expansion of the surveillance state at the direct expense of civil liberties. We strongly urge FinCEN to reconsider this dangerous approach. However, we hope to provide a more focused response on the overbreadth of the activities that are included as CVC mixing activities in the Proposal by providing a functional perspective.

I. Overbreadth in the Definition of CVC Mixing Represents an Overstep of Authority.

FinCEN has asked for comments on the scope of the class of transactions covered. CVC mixing is defined in the Proposal 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"[17] and without reference to intent or degree of success in doing so. This low bar for inclusion operates in conjunction with an expanded concept of 'mixing'.[18] The Proposal also includes within the definition the following wide-ranging and non-exhaustive list of types of on-chain behaviors that constitute CVC mixing, including transactions "such as: (1) pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts;[19] (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; or (6) facilitating user-initiated delays in transactional activity."[20]

[14] Proposal at 2.
[15] Proposal at 75 (emphasis added).
[16] As a matter of common sense, just because a criminal uses a bakery as a front to launder money, it does not make sense to declare bakeries a high risk category or necessitate a presumption that they are of primary money laundering concern.
[17] Proposal at 30.
[18] See *infra* discussion in Section I(A).
[19] *Id*.
[20] Proposal at 75-76.

Though we would have significant reservations around the erosion of privacy inherent in this Proposal if it were just focused on 'mixers' as a continuation of the expanded definition from the Tornado Cash designations,[21] it is important to note that many of the cited activities are not "anonymity enhancing tools".[22] They are not privacy-focused and some do not serve a privacy purpose whatsoever, let alone are undertaken with the intent to obfuscate. As the impetus for the Proposal is FinCEN's "concern[] that CVC mixing makes CVC flows untraceable",[23] it would be crucial to confirm the covered activities actually further this purpose. In fact, notwithstanding the Proposal's baseless characterization of these as being "critical" to criminals, the vast majority of the activities covered by the Proposal do not make CVC flows untraceable. They instead have legitimate and everyday purposes.[24] Along these lines, our comments will focus on the scope of the activities captured and provide factual context and technical corrections on some of the premises in the Proposal to better inform rulemaking understandings. Essentially, as drafted, the Proposal amounts to a thresholdless SAR regime where suspicion is presumed for use of the technology. **If FinCEN intended this scope, FinCEN should undertake a rulemaking stating this intention with proper notice and supporting economic analysis**.

For instance, while FinCEN is required to consider "the extent to which such class of transactions is used to facilitate or promote money laundering",[25] we note a stunning lack of citations and statistical support in the underlying assertions in the Proposal.[26] While the Proposal acknowledges it uses a "broad" definition of CVC mixer,[27] FinCEN also "deems the breadth of this definition to be necessary" due to "the nature of

[21] *See infra* discussion in Section I and accompanying notes regarding the ever-lowering bar to 'facilitating obfuscation', which to date, despite historical expansion, only covered a narrower set of activities within prong (1) of the Proposal's definition.

[22] *See* Proposal at 75-75 expanding any historically held definition of mixers to now cover any behavior or technology, whether or not there is an intent (let alone the sole intent) to obfuscate. *Cf.* discussion of 'mixers' as a type of anonymity enhancing tool and 'CVC mixing' as "intended to obfuscate transactional information. Proposal at 7.

[23] Proposal at 21.

[24] The point that crypto is not a critical currency or conduit for criminals (let alone the covered activities) has been repeatedly reinforced over time. Most recently, experts have cited that the critical channels to Hamas's funding resources are (i) "State funding, which is transmitted ***mainly by*** cash, cross-border payments, Hawala, trade-based terrorism financing, money exchanges and banks", (ii) its business portfolios, "including real estate and investments", (iii) humanitarian aid, "which is misappropriated to and stolen for its own activity", and (iv) fundraising activities, "including through social media platforms and crowdfunding campaigns." And with respect to prong (iv), although crypto was cited as a method, alongside money " transmitted via bank accounts [and] payment services" (emphasis added). Hamas announced that it was ceasing to accept Bitcoin in March of 2023 due to its traceability and 'hostile' activities against donors before additional crypto fundraising accounts were frozen later in the year. Written Testimony of Dr. Shlomit Wagman, Oct 25, 2023, "Combating the Networks of Illicit Finance and Terrorism," before the Senate Committee on Banking, Housing, and Urban Affairs, available at https://www.banking.senate.gov/imo/media/doc/wagman_testimony_10-26-23.pdf (citing Reuters, Hamas Armed Wing Announces Suspension of Bitcoin Fundraising, Apr. 28, 2023, https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ and Reuters, Israel Freezes Crypto Accounts Seeking Hamas Donations, Police Say, Oct. 10, 2023, https://www.reuters.com/technology/israel-freezes-crypto-accounts-seeking-hamas-donations-police-say-2023-10-10/).

[25] Proposal at 3.

[26] FinCEN cites a single 2022 Chainalysis blog post to back up this assertion instead of robust year over year statistical analysis that ties what FinCEN now broadly describes as "mixers" to illicit activity. See Proposal note 57 and accompanying discussion. The Proposal relies heavily on this single source. As has been pointed out repeatedly Chainalysis and other similar companies are each single private actors in the space that have vested interests in creating alarm around issues that drive their core businesses. See, e.g., Sam Lyman, How Misinformation On Hamas And Crypto Fooled Nearly 20% Of Congress, Forbes, November 8, 2023 ("**Forbes Article**") , available at https://www.forbes.com/sites/digital-assets/2023/11/08/how-misinformation-on-hamas-and-crypto-fooled-nearly-20-of-congress/?sh=6a30ab808270 (stating it is important to "[k]eep in mind that the core business of Chainalysis and Elliptic is to help governments identify illegal activity on the blockchain. These companies have a strong financial incentive to emphasize the link between crypto and criminal activity").
Chainalysis has also admitted to data validation issues in court. See, for example, the Declaration of Elizabeth A. Bisbee, Director of Investigation Solutions for Chainalysis Government Solutions, a wholly owned subsidiary of Chainalysis Inc., filed July 18, 2023, available at https://www.courtlistener.com/docket/59988850/149/1/united-states-v-sterlingov/ ("[h]istorically, Chainalysis has not gathered and recorded in a central location false positives /false negatives because there is design to be more conservative in the clustering of addresses. In response to the Court's inquiry, Chainalysis is looking into the potential of trying to collect and record any potential false positives and margin of error, but such a collection does not currently exist."); *see also* reports citing that Bisbee also testified that "she was "unaware" of scientific evidence for the accuracy of Chainalysis' Reactor software used by law enforcement in an unreleased transcript of a June 23 hearing shared with CoinDesk." available at https://www.nasdaq.com/articles/chainalysis-investigations-lead-is-unaware-of-scientific-evidence-the-surveillance.

[27] Proposal at 31.

CVC mixing".[28] In doing so, FinCEN makes several logical leaps that their conclusions would likely be statistically supported that the treatment that they are arbitrarily imposing here will be impactful. Yet FinCEN has failed to show statistical support for the need for this rulemaking as it relates to the covered activities. FinCEN admits in the Proposal that the need is based on a hunch as "only a portion of the activity in the CVC ecosystem with exposure to CVC mixing is captured by BSA reporting[29] [and] [a]s a result, FinCEN assesses that high-risk deposits into CVC mixers are *likely* underreported, and the percent of CVC tied to illicit activity is *likely* higher."[30] Aside from thin data from private companies,[31] FinCEN offers as support simply a passing reference that criminals have used some of the broader cited activities.[32] **FinCEN fails to assert that this use (again under the expanded definition) is statistically significant as a function of total transaction volume. It also fails to cite any statistics that support that the use of mixers for CVC mixing activity**, as described in prong (1) of the definition in the Proposal, is going up for illicit activities as a percentage of total on-chain transactions and the enforcement actions to date have failed to discourage the use of mixers in the traditional sense, let alone the expanded categories.[33] In fact, one of FinCEN's sources for statistical analysis, in its 2023 reports, states that these types of activities were down almost across the board as a function of total on-chain activity.[34] This leads us to question the impetus for both the expansion of prong (1) and the inclusion of prongs (2) through (5).

Given this proposed rule is being promulgated under special statutory authorization focused on money laundering activities, it seems problematic that the proposed rule encompasses a broad swath of activity that does not meet the legal or even the functional definition of money laundering. Our primary concern is this overstep of statutory authority. As it relates to the definitions, we are particularly troubled as to what the Proposal considers to be CVC mixing activities, expanding prong (1) and adding four new types of activities to capture all on-chain behaviors, from the basic operation of smart contracts and simple transactions to mundane features, and tools without privacy applications. These new categories, which have multitudes of use cases with legitimate business purposes, are nevertheless now being swept into the definition of CVC "mixing". Additionally, various on-chain activities that are widely considered to be security good practices are being framed by the Proposal as having the effect of obfuscating. The inclusion of these activities paints a sheen of suspicion over the broad swath of U.S. users of permissionless technology - the commonality between them not being criminal intent but instead being a part of the younger generation of Americans that embrace technology and see it as vital to their economic future.[35]

---

[28] *Id*.

[29] Without analysis on other regimes or methodologies that could capture the intended data - and by intended data, we mean mixing activities tied to illegal acts.

[30] Proposal at 19 (emphasis added).

[31] *See supra* note 26 (referencing reliance on Chainalysis and statistics related to mixers of the type described infra in notes 36-37 and accompanying discussion).

[32] Proposal at 8-10. *See also*, *infra* notes 49 and 62 and accompanying discussion.

[33] *But see* on-chain data available at https://dune.com/hildobby/tornado-cash (an analytics dashboard showing the drop in TVL post-enforcement) and see supra note 8 (describing on-chain data showing the impact of the Tornado Cash regulatory actions on Tornado Cash activity).

[34] See https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/ ("**Chainalysis 2023 Mid-Year Report**") and https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ ("**Chainalysis 2023 Year End Report**") Total on-chain activities are based on "funds changing hands" and Chainalysis excludes from the total any "type of transaction that Chainalysis removes "would not count as an economic transaction between distinct economic actors" from their count of on-chain activity. Note that FinCEN does not, which will increase the inbound volume of transactions under the Proposal that need to be vetted and decreases the cited percentages of prevalence of illicit activity. *See* discussion of false positives and follow-on effects in Section III(B) below.

[35] Studies have consistently found that adoption skews significantly younger, with one study using a sampling of 2021 data to find "[n]early 94% of cryptocurrency buyers are in the age range of 18-40, with Gen Z and Millennials making up the majority" *See* Stilt, Vast Majority of Crypto Buyers Millennials & Gen Z (Mar. 2021), available at https://www.stilt.com/blog/2021/03/vast-majority-crypto-buyers-millennials-gen-z/. Another 2022 report indicates adoption originating from younger demographics, with "40% of 18 to 35-year-old consumers expressing an intent to use cryptocurrencies — such as bitcoin (BTC), ether (ETH), and stablecoins — to pay for goods or services within the next 12 months". *See* CryptoSlate,

Beyond applying to just the younger generation, good security and privacy practices are essential to everyone transacting in our increasingly online world.

A. Expansion of CVC Mixing to include activities that involve "[p]ooling or aggregating CVC from multiple persons, wallets, addresses, or accounts"

Mixers are typically conceptualized as services with the explicit purpose and end-goal of obfuscating user funds.[36] In its 2022 National Money Laundering Risk Assessment (the "**2022 Risk Assessment**"), FinCEN described 'mixers as "websites or software *designed to conceal or obfuscate* the source or owner of virtual assets." Though expanding the definition, OFAC described Tornado Cash as "a virtual currency mixer that operates on the Ethereum blockchain and *indiscriminately facilitates anonymous transactions by obfuscating* their origin, destination, and counterparties, with no attempt to determine their origin. Tornado receives a variety of transactions *and mixes them together* before transmitting them to their individual recipients."[37] Both descriptions imply an intent, a purpose, and end-result of facilitating anonymization.

However, in the Proposal, the scope has been drastically expanded to cover the functional equivalent of *any* company account. Under this standard, start-ups and operating businesses collecting capital contributions from founders or fundraises from investors into a entity level-account, amounting to pooled vehicles and funds transacting on-chain, would be subject to the rulemaking under a presumption that the business was attempting to "obfuscate the identity" of the parties involved. This new reporting regime would likely overlap with other simultaneous and duplicative reporting obligations such as, among other things, the Corporate Transparency Act compliance requirements, the new IRS 6050I reporting regulations on payments, and existing AML and other compliance obligations that would be applicable depending on the context. Beyond transactions involving multiple parties, this could capture a variety of basic and benign legitimate transactions from a single user organizing their finances – like funding a CEX account from multiple self-custodied wallets, aggregating SOL dust from multiple wallets to consolidate $20 in holdings and transferring multiple assets to a custodian for cold storage.[38]

B. Inclusion of "exchanging between types of CVC or other digital assets"[39]

Representing a new prong of mixing activity is the inclusion of "exchanging between types of CVC or other digital assets"[40] within the Proposal's definition of CVC mixing. However, what the Proposal fails to acknowledge or appreciate is that exchanging CVC or digital assets, referred to in the Proposal as "chain hopping" to erroneously invoke pernicious intent, is a basic reality and necessity in transacting on-chain.

40% of Youngsters Want to Use Crypto for Payments: Research (2022), available at https://cryptoslate.com/40-of-youngsters-want-to-use-crypto-for-payments-research/.

[36] *See e.g.* description provided in Adam Doupe, Bitcoin Mixers: Anonymity Analysis and Deanonymization Strategies (2019), available at https://adamdoupe.com/publications/bitcoin-mixers-fc2021.pdf. *See also* U.S. Department of the Treasury, Financial Crimes Enforcement Network, 2022 National Money Laundering Risk Assessment (2022), available at https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf (hereinafter the "**2022 Risk Assessment**").

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

[38] *See* below discussion of wallet use in Section II(A)(ii). *See supra* Section I discussion on the lack of support and accompanying notes. It is also likely designed to capture DeFi activities such as the use of liquidity pools as being of primary money concern while failing to offer proof that the rulemaking is necessary or helpful to the stated goal. We also echo the points raised in the comment letter from DeFi Education Fund on this point (emphasizing that including them contradicts the 'obfuscation' limitation of the definition).

[39] Proposal at 31.

[40] Given one of the assurances from FinCEN around the narrowness of the rule, as it only encompasses CVC transactions with covered financial institutions, the fact that non-CVC was included in this category is not lost on us. *See infra* Section 3(B) below for more discussion on the purported narrowness of the rulemaking not being supported by fact.

Cross-chain transfers are easily traceable on-chain,[41] the transfers themselves occur on public blockchains, and transaction times and amounts can be easily linked using forensics. This activity is not an effective typology of money laundering given that these transfers take place openly on a public and searchable ledger. Rather, cross-chain transfers instead arise out of normal behaviors for and necessities of transacting on-chain. This is largely because there are upwards of one thousand different blockchains (L1s or "chains"),[42] each of which can constitute siloes for on-chain activity, which has negative follow-on effects for users, developers of Dapps, and the crypto ecosystem at large.

Solving for interoperability, or the ability for chains to talk and process information passed between each other, has been a challenge that technologists have been trying to solve for years. Blockchains, by their nature, are closed-loop systems for data that rely on complex and often bespoke processes to verify data within their native ecosystems.[43] Thus, attempting to introduce external data and inputs and designing the best means to verify and validate such inputs and data has been an area of intense debate and ideation.[44] Ideation on how to best accomplish interoperability and facilitate cross-chain transactions continues to this day, with fierce debates on the path forward, from the proliferation of EVM chains[45] to the Cosmos ecosystem itself[46] which makes interoperability part of their core design and value proposition to the ongoing design of swaps and cross-chain bridges across other L1s to help facilitate cross-chain transactions. Improving interoperability can mean the difference between a decentralized application ("dapp") deploying and maintaining one instance versus needing to develop, deploy, and maintain an instance on each chain.[47]

Crypto, as an industry, is still engaged in continuing to develop infrastructure to improve interoperability and thus improve user experience – solving for the ability to 'hop' between chains is an express and healthy goal of crypto development.[48] The market has yet to determine which of these competing methodologies optimally solves the underlying issues with the least negative externalities. The Proposal seeks to put its thumb on the scale by disincentivizing swaps and erecting arbitrary barriers by capturing user on-chain behavior as they seek to switch chains, exacerbating silo effects and fragmentation. It captures both 'chain-hopping' between L1s as well as the use of L2s to save gas fees. Gas fees are often-cited by critics as a blocker for consumer adoption; and many developers have spent years working to reduce gas costs, the

[41] *See, e.g.*, Saad Yousaf et al., Tracing Transactions Across Cryptocurrency Ledgers, 28th USENIX Security Symposium, August 2019, https://www.usenix.org/system/files/sec19-yousaf_0.pdf (demonstrating the ability as of 2019 to capture "complex transactional behaviors" and trace their activity across ledgers, with implications for criminals trying to "obscure their flow of money").

[42] Estimates cite the existence of 1,000s. *See* The Current State of Interoperability between Blockchain Networks, EU Blockchain Observatory and Forum, November 2023, available at https://www.eublockchainforum.eu/sites/default/files/reports/EUBOF_Interoperability%20Report-30112023.pdf ("**Interoperability Report**"), at page 5.

[43] *See Id.* for further background on interoperability challenges and current solutions being developed.

[44] This work continues, including the development of the modular thesis, as seen in Celestia, which attempts to solve scalability by reenvisioning L1 architecture, which some critics note increases complexity and dependency on bridges. *See, e.g.,* Multicoin Capital, "The Hidden Costs of Modular Systems" (Aug. 15, 2023), available at https://multicoin.capital/2023/08/15/the-hidden-costs-of-modular-systems/.

[45] "An Ethereum Virtual Machine (EVM) Chain is a blockchain network that can execute smart contracts and process transactions in a manner compatible with Ethereum's own computational engine, the EVM. This compatibility facilitates a unified development environment for decentralized applications (dApps) and smart contracts, streamlining user experience across various platforms." What are EVM Chains, available at https://www.datawallet.com/crypto/evm-chains.

[46] See Paradigm, A Cosmos Thesis, https://www.paradigm.xyz/2021/04/a-cosmos-thesis (describing the interchain thesis and benefits of Cosmos).

[47] The latter being a significant impediment to moving the space forward, where, instead of efforts to improve security, infrastructure, user experience, features, etc, developers would be spending all their efforts building and maintaining separate implementations for each chain. See below discussion of one of the core features of smart contract composability and the open source movement is the ability to leverage building blocks.

[48] *See, e.g.*, Interchain Foundation, "Eli5: What is IBC?" available at https://medium.com/the-interchain-foundation/eli5-what-is-ibc-def44d7b5b4c (stating the goal of IBC is to "solve the problem of blockchains existing as silos with limited interaction. Interoperability between blockchains is necessary for maximal value accrual. Each blockchain caters to one or more specialized use cases. If these use cases cannot be leveraged across multiple blockchains, it severely handicaps their utility. The breakthrough that the internet provided is that information can easily flow across different parts of the world with ease. Similarly, the utility of different blockchains need to be freely accessible across multiple platforms").

results of any of such efforts would be bound to be captured by at least one prong of purported 'mixing activities'.

Attaching an unprecedented veil of regulatory suspicion and presumption to these behaviors is categorically irrational and produces high costs. Especially for the behavior captured. Much like one might exchange Japanese Yen for USD as one travels to the U.S. for a business trip (because trying to transact in Yen would not be particularly effective in the U.S.), you might look to exchange L1 tokens you hold to engage in transactions on another chain - purely as a function of leaving one ecosystem and desiring to transact (and have the transaction go through) in the next. Yet, one does not infer criminal activity from foreign exchange transactions. This is because, although criminals certainly engage in them and they certainly occur, criminal forex transactions are statistically insignificant as compared to those that are legitimate and for benign everyday purposes. Likewise, while some cross-chain transactions may be intended to further criminal purposes, it does not logically follow that most or even many transfers between chains involve criminal activity.

We note that the inclusion of this type of activity creates an uneven regulatory playing field as FinCEN has not applied this surveillance rule to all forex transactions. It would not make sense to do so from a policy perspective as it would be too noisy a signal for surveillance purposes, it would have too high costs and be too disruptive to international trade, and it would be an undue burden on commerce. For the same reasons, these requirements should not apply to the nascent crypto industry - they would impose an undue burden and even higher costs than those that would be incurred in forex because of the amount of swapping needed before the interoperability issue discussed above is solved. The result for crypto would indeed be dire; it would turn an already strained, in-development user experience to one that is no longer viable.

Aside from the basic types of transactions described above, "Chain Hopping" patterns can be many things, none of which constitute money laundering.[49] Additional examples include:

- "Hopping" can encompass a variety of "swap" behaviors achieved through primitives to provide benefits similar to a forex conversion transaction while reducing negative externalities like transaction costs or complicated multi-step processes, from atomic swaps to using some other platform that allows for native swapping without a bridged or wrapped asset.

    - Atomic swaps enable peer-to-peer exchanges of digital assets across chains.[50] Atomic swaps, such as those on Synthetix, operate to enable trading from one asset to another by utilizing synthetic assets as intermediating assets.

    - Another method of executing swaps would be THORChain synths, which (among other models) seek to improve user experience by avoiding potentially significant transaction (gas) costs

[49] In fact, the 2022 Risk Assessment only makes a passing reference to the behavior without going as far to cite any statistical basis for it to be included alongside what is traditionally seen as CVC mixing. *See* 2022 Risk Assessment, *supra* note 36 at page 42 ("citing that "[r]ecent law enforcement investigations involving virtual assets have uncovered chain hopping (moving assets from one blockchain network to another via an exchange, swap, or "wrapped" asset), and some of this activity has involved the use of smart contracts and other DeFi services.").

[50] For an explainer, *see* Chainlink, Education Hub, Atomic Swaps, https://chain.link/education-hub/atomic-swaps (describing atomic swaps as enabling "peer-to-peer exchanges of crypto tokens across different blockchain networks that only execute if both parties each deposit a predetermined amount of tokens to the exchange contract. This enables any two users to swap digital tokens without relying on a third party to facilitate the transaction, thereby reducing counterparty risks").

and frictions involved in swaps while on THORChain until the user has finished the transaction and withdraws to the chain they choose.[51]

- Similarly, liquidity aggregators, such as ParaSwap, use price discovery and routing algorithms[52] to achieve optimal pricing for token swaps, allowing users to access multiple sources of liquidity and execute cross-chain transactions with minimal slippage.

These functions can provide highly customizable experiences putting the control in the user's hands or be used on the back-end to help users get a similar user experience ("UX") to trading assets in a Fidelity or Vanguard Account despite trading across chains where transacting among different assets is a seamless experience.

- Other basic on-chain transactions are accomplished by cross-chain activity, such as:

- Liquid staking allows a user to stake an asset such as ETH and receive tokens representing their staked tokens and accrued yield through rebasing tokens (such as stETH) or non-rebasing (such as rETH) allowing consumers to participate in staking activities to secure the blockchain in proof of stake ("PoS") models without the high barriers to entry.[53]

- Wrapping ETH for compatibility with ERC-20 standards to use in a similar fashion as other ERC-20s, including for something as basic as purchasing an NFT on OpenSea.[54]

- Apart from crypto native applications, the 'chain-hopping' behavior can be analogized to more traditional behaviors like high frequency, hedge fund, and arbitrage-focused trading that serve the important function of price discovery to maintain efficient prices across platforms. Similarly, market makers serve a vital function in the cryptocurrency markets by engaging in this type of 'chain hopping' behavior.

We have seen a lot of rhetoric against permissionless technology, often divorced from fact. This has resulted in overly onerous rulemaking and legislative proposals that attempt to regulate peer-to-peer transactions as if they have inherent illicit intent. Since the goal of the Proposal is purportedly to "counter the efforts of terrorist groups, such as Hamas and Palestinian Islamic Jihad, that engage in violence against innocent civilians" together with other anti-money laundering and sanctions evasion activities,[55] it necessarily follows that there must be extreme risk caused by the covered transactions and extremely insufficient means

[51] *See* THORSwap, Synthetic Assets, https://docs.thorswap.finance/thorswap/ecosystem/thorchain/synthetic-assets. For more on how synths operate on THORChain and the value add to the user, *see* Can Gurel, The Resurrection of THORChain, April 11, 2022, https://members.delphidigital.io/reports/the-resurrection-of-thorchain#key-takeaways ("Prior to synths, one could think of THORChain as an exchange where users were forced to deposit, swap, and withdraw assets, bearing expensive gas costs each time they wanted to make a trade. With synths, users have the option to deposit and do as many trades as desired on THORChain, while also keeping the option of being able to withdraw native tokens to their chain of choice. Naturally, this is a much cheaper mode of operation and has so far attracted significant traction").

[52] For a further description of the functionalities, see Paraswap Documentation, https://doc.paraswap.network/.

[53] For more background see, e.g., "What is Liquid Staking", https://www.ledger.com/academy/topics/defi/what-is-liquid-staking.

[54] *See* OpenSea Primers, How do I make an offer?, available at https://support.opensea.io/hc/en-us/articles/360063518053-How-do-I-make-an-offer-on-NFTs-; What is WETH and how to I get it, available at https://support.opensea.io/hc/en-us/articles/360063498293-What-s-WETH-How-do-I-get-it-

[55] Proposal Press Release *supra* note 3 (citing a goal to counter the efforts of terrorist groups, such as Hamas and Palestinian Islamic Jihad, that engage in violence against innocent civilians; the efforts of ransomware criminals targeting critical infrastructure; and the efforts by state actors and their supporters to evade U.S. and global sanctions).

available to law enforcement to address such risks. However, despite the release accompanying the Proposal describing CVC mixing (presumably as now broadly defined in the Proposal) as offering a "critical service that allows players in the ransomware ecosystem, rogue state actors, and other criminals to fund their unlawful activities and obfuscate the flow of ill-gotten gains," FinCEN has alleged that illicit actors engage in the enumerated activities[56] without providing evidence of any significant or material use by these actors, much less a critical or overwhelming reliance.[57] Indeed, although FinCEN noted a rise in laundering involving crypto in its 2022 Risk Assessment, the report also found "the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods".[58] Treasury's April 2023 Illicit Finance Risk Assessment of Decentralized Finance once again acknowledged that "money laundering, proliferation financing, and terrorist financing ***most commonly occur using fiat currency or other traditional assets as opposed to virtual assets***." What's more, a source of FinCEN's statistical data has reported that as of mid-2023, by most metrics, illicit use of crypto had ***gone down*** year over year.[59] The Proposal is the result of an overreaction in approach due to rhetoric as opposed to a measured attempt based on facts. For instance, in the weeks immediately preceding the Proposal, a U.S. Senator decided it would be politically expedient to push a narrative that Hamas leveraged crypto fundraising to raise more than $100 million. This baseless claim was easily and incontrovertibly disproved by fact-based research made possible by on-chain analytics[60] and Hamas was later found with suitcases of cash.[61] Likewise, although the Department of Justice may allege "money laundering" in a complaint involving virtual currency, it doesn't follow that all similar or categories of behaviors associated with transacting in virtual currency are in aid of a crime or have some sort of malicious intent.[62] FinCEN fails to cite the statistical significance between the cited but thinly supported 'prevalence' of chain hopping in money laundering as a function of total chain hopping activity for this reason - it is statistically insignificant.[63] Further, "chain hopping" between blockchains by itself doesn't fit the formal definition of layering, placement, and/or integration in money

[56] "FinCEN based this assessment on information available to the agency, including both public and ***non-public reporting,*** and after thorough consideration of each of the following factors: (1) that transactions involving CVC mixing often occur within, or involve, jurisdictions outside of the United States; (2) that CVC mixing is used to launder proceeds of large-scale CVC theft and heists, and support the proliferation of WMD, in particular, by the DPRK; and (3) that CVC mixing is similarly used by ransomware actors and darknet markets to launder illicit proceeds." Proposal at 13 (emphasis added). As referenced in supra note 31-32 and accompanying discussion, the data cited is thin - if there is additional and substantial data, we have not had the opportunity to see it.

[57] According to a former Human Trafficking Finance Specialist in the Money Laundering and Asset Recovery Section of the U.S. Department of Justice (DOJ) testifying recently before Congress, "the traditional financial system remains a big avenue for illicit actors to evade sanctions and launder money. There is no means of exchange that is more anonymous than cash, which truly leaves no footprint, and there is no blockchain for cash." Jane Khodarkovsky, Written Testimony before the U.S. House Financial Services Committee, Subcommittee on Digital Assets, Financial Technology and Inclusion, "Crypto Crime in Context: Breaking Down the Illicit Activity in Digital Assets" (Nov. 15, 2023), available at https://docs.house.gov/meetings/BA/BA21/20231115/116579/HHRG-118-BA21-Wstate-KhodarkovskyJ-20231115.pdf.

[58] 2022 Risk Assessment *supra* note 36 at 41.

[59] *See* Chainalysis 2023 Mid-Year Report and Chainalysis 2023 Year End Report *supra* note 34. According to the Chainalysis 2023 Mid-Year Report "[t]hrough the end of June, crypto inflows to known illicit entities – not including inflows to entities that have been sanctioned or subject to special measures – are down 65% compared to where they were at the same time in 2022. Inflows to risky entities (made up primarily of mixers and high-risk exchanges) are down 42%. Of course, transaction volumes are down across the board, but declines are much less severe for legitimate services, which have seen just a 28% drop in inflows. In other words, there's been a market pullback, but illicit crypto transaction volume is falling much more than legitimate crypto transaction volume." The year-end numbers also reflect an overall year over year decline.

[60] The episode was driven by politicians pushing "a bloated number that bore little resemblance to reality" that, even after being disproved "continued to drive policy conversations in Washington." See Forbes Article *supra* note 26. Elliptic released a response correcting the false assertion that their data showed that $130 million was raised in crypto, *see* Elliptic, "Setting the Record Straight on Crypto Crowdfunding by Hamas," available at https://www.elliptic.co/blog/setting-the-record-straight-on-crypto-crowdfunding-by-hamas (clarifying that "[t]here is no evidence to suggest that crypto fundraising has raised anything close to this amount, and data provided by Elliptic and others has been misinterpreted" and discussing Hamas' decision to discontinue all crypto donations because of its traceability "illustrates the weakness of crypto as a terrorism fundraising tool."

[61] *See* discussion in *supra* note 24.

[62] Even prong (1) cannot reasonably be described through this lens without an intent to obfuscate. *See supra* Section I(A) and accompanying notes for a discussion of the business activities that could be considered in-scope.

[63] Proposal at 18 (basing the conclusion on a 2021 data set based on a six-month sampling of 635 ransomware SARs based on Bitcoin activity (not referencing which of these were actual criminal activity) and for uncited reasons determined the behavior to be "prevalent".

laundering.[64] As discussed herein, on-chain transactions provide more traceability and more of a 'paper trail' than cash transactions.[65] Far from being critical to money laundering and attempts at obfuscation, these transactions leave a permanent and public record of the transactions.

All stores of value and financial assets carry the same risks as crypto but none are similarly singled out for this regulatory treatment. At the same time, as an implicit acknowledgement of how onerous the rulemaking will be, the only carveout from the definitions of CVC mixing activities are the exact same transactions when done by banks and intermediaries.[66] The Proposal's goal on this prong seems to be to erect barriers to adoption for non-intermediated transactions as well as an attempt to re-enshrine rent-seeking by financial intermediaries by driving consumers to exchanges to convert to USD and incur tax repercussions before incurring more fees to buy the desired tokens in order to change chains.

C. Inclusion of "using programmatic or algorithmic code to coordinate, manage or manipulate the structure of a transaction".

The Proposal inappropriately includes ordinary smart contract functions in the definition of virtual currency mixing, like "using programmatic or algorithmic code to coordinate, manage or manipulate the structure of a transaction." All smart contracts are designed to engage in exactly the behaviors this prong includes - using code to structure and execute transactions.[67] There is no privacy feature inherent in this activity other than these transactions being carried out on-chain. Thus, performing the same functions on a blockchain as you would in the traditional sense through manual and paper processes should not subject you to heightened scrutiny.

Examples of smart contracts coordinating and managing transactions include all manner of on-chain behaviors, such as, but not limited to: (1) using smart contract escrows (including self-executing release if conditions are met); (2) setting-up and execution of transactions through multisignature wallets; (3) automating payment splits based on predefined rules (from multiple CEX accounts to automating royalty payments to creators with digital art purchases); (4) code automating the carrying out of auction processes and enforcement of bidding rules; and (5) facilitating automated micropayments when conditions are met such as micropayments for personal data shared with a website to the owner of the data.

Composability allows developers to take existing code (such as the basic use case functions above) and reuse it, repurpose it, modify it, and combine it with other code to make something altogether new. A goal of the open source movement is to build upon existing building blocks and combine them to design applications fit for purpose. In this manner, the above transactions incorporate helpful features and functions made possible by smart contracts, including the following design patterns:

---

[64] *See e.g.*, Financial Crimes Enforcement Network (FinCEN), "Prevention of Illicit Money Services Businesses" (2011), at 2, available at https://www.fincen.gov/sites/default/files/shared/prevention_guide.pdf (describing layering as "separating the illegally obtained money from its criminal source by layering it through a series of financial transactions, which makes it difficult to trace the money back to its original source" and structuring as transactions such as "coercing or bribing employees not to file proper reports or complete required records, or by establishing apparently legitimate "front" businesses to open accounts or establish preferred customer relationships."

[65] *Id*. at 2 citing as key, criminals attempting to not leave "paper trails."

[66] *See* Proposal at 31 ("[t]his definition excepts the use of internal protocols or processes to execute transactions by banks, broker-dealers, or money services businesses, including VASPs, that would otherwise constitute CVC mixing").

[67] *See,* among other explainers, Gemini Cryptopedia - Smart Contracts, available at https://www.gemini.com/cryptopedia/smart-contract-examples-smart-contract-use-cases (describing a smart contract as "self-executing code that carries out a set of instructions, which are then verified on the blockchain. They are a core technological element of many decentralized applications (dApps). A key characteristic of smart contracts is that they are trustless, meaning they can reduce or even eliminate the need for third-party intermediaries."); https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718_0.pdf

i. **Time delays or timelocks** - these can serve a wide variety of purposes such as delaying execution of a governance proposal until a certain threshold has been reached (ie. a 72-hour window) or implementing a vesting condition, streaming payments or transfer restrictions; they can also be used as speed bumps to guard against price manipulation in DeFi lending; and things like hash time-locked contracts are used to ensure that both parties fulfill their obligations in an exchange within a specified time frame - if the conditions are met, the assets are automatically exchanged and if not met, the transaction is canceled.

Time-delays can also serve a compliance function, as demonstrated by the Privacy Pool model, which centers on the objective of maintaining pool anonymity among a pool of participants while excluding sanctioned actors and illicit funds from innocent and compliant privacy pools and leverages a time delay on introduction of new transactions to the anonymity set, of a week or number of weeks, to allow time to identify stolen or sanctioned funds and ensure they are not included in the "compliant" association set. Under the Proposal, this model would still meet the aggregation prong and this model of balancing privacy with compliance would be disincentivized. We urge the development of guidance that preserves the right to privacy while advancing the important policy goals of combating terrorism and illicit activity. However, on this component alone, it is an unfortunate irony that FinCEN's proposed rule discourages the use of smart contract-based compliance tools that actually help *prevent* money laundering activity.

ii. **Additional Programmatic Features That Improve Asset Security**. Time delays at different stages of a transaction can serve a variety of security purposes. Inbound delays stop attacks by preventing crediting bad deposits that get unwound. Next, processing delays can prevent market manipulation attempts at the expense of other users. Finally, outbound delays prevent attackers from being able to quickly siphon out funds. In addition to time delays, the following additional programmatic features that improve security and thus user safety:

- Rate limits - operating similarly to the time delay, these are used to limit withdrawals by setting caps or limiting the amount of token mints, slowing the pace by which bad actors can withdraw funds and limiting the impact of hacks.
- Automated circuit breakers for events such as automated alerts for suspicious transactions (volume, source, sharp increases in particular behaviors such as withdrawals etc.)
- Automated pauses if conditions are met, such as a critical bug is discovered, that prevent harm from an exploit.
- Wrapper tokens that wrap other tokens to prevent theft in the case of a discovered bug.[68]

These smart contracts and functions are technological building blocks for increased security. Moreover, encouraging composability enhances security through leveraging modularity because developers can extend or modify a smart contract's functionality by integrating code stored elsewhere through something called contract inheritance. This allows developers to reduce the amount of new code they must write and

[68] *See e.g. supra* note 13.

allows them to integrate existing code that is the product of extensive code reviews and vetting as it has been deployed and tested widely by the broader open-source community.[69]

D. Inclusion of "facilitating user initiated delays in transaction activity".

The next category of activity that is included is perplexingly more granular[70] while overlapping with the above category capturing the use of smart contracts more generally, but again, "facilitating user initiated delays in transaction activity" captures features intended to benefit the user *without* adding privacy-preserving features. "User-initiated delays" are not typically or necessarily for the purpose of obfuscation, but rather can be used to serve a variety of important functions.

i. Programmable Money. For example, time delays are used to provide streaming payroll payments to employees or contractors, thus giving workers more immediate access to the funds without the need for intermediaries that can introduce fees and processing delays. Instead, workers have real-time access to funds that they have earned, possibly reducing the dependency such workers and their families may have on more predatory services such as payday lenders and salary advances in times of crisis. This concept can be expanded to automate grant payments upon the achievement of milestones and automate vesting over time and provide certainty to the recipient as a means to enforce contractual commitments without relying on legal enforcement mechanisms, which can be prohibitively costly. Implementations of this are Hedgey and Sablier,[71] where a user can select the time of time delay desired to implement the stream with a high degree of composability - from linear streams that provide payments at a rate per second to a cliff or more traditional unlock that is followed by a stream.[72]

Ironically, a result of the rulemaking would be to make workers using off ramps for their paychecks - an incredibly mundane but important and essential activity - subject to suspicion, being frozen, being reported and undermining the inherent consumer benefits.

ii. Trading Applications. Another use case of user-initiated delays is for users seeking to employ a trading strategy, such as a TWAP strategy,[73] for better price discovery and another can be for a user to introduce time delays to reduce slippage for the benefit of the user. For the trading strategy use case, we have also seen implementations of trading strategies through smart contracts such as Cowswap's TWAP[74] primitive and Jupiter's DCA mode.[75] Cowswap TWAP orders "allow traders to spread their trade

---

[69] *See, e.g.*, OpenZeppelin Blog, "Open Source Collaboration in the Blockchain Era: EVM Packages" (available at https://blog.openzeppelin.com/blog/open-source-collaboration-in-the-blockchain-era-evm-packages).

[70] We can only guess at its inclusion but it might be a remnant of how older centralized Bitcoin mixers functioned, utilizing time delays along with randomized withdrawal amounts (and wallet addresses), to help anonymize the transaction. This would still presume a more expansive definition of 'user-initiated' delays to fit under this prong as the delay would not be within the control of the user. However, the aggregation and an intent to obfuscate should still be captured by prong (1). See, e.g., https://bitcoinwiki.org/wiki/bitcoin-fog.

[71] *See* Hedgey Finance, "Introducing Hedgey V2" (available at https://hedgey.finance/blog/introducing-hedgey-v2) (a no-fee infrastructure project available on Ethereum and most EVM-compatible chains) and Sablier Protocol Documentation, "Concepts" (available at https://docs.sablier.com/concepts/sablier-protocol) (which does not charge fees for ERC-20 assets, and the only fees in this implementation are gas fees. Sablier has multi-chain implementations and is currently on 9 chains).

[72] *See* Sablier Gallery available at https://app.sablier.com/gallery/ (displaying the variety of streaming payment flows available for a user to choose from).

[73] In crypto, time weighted average price (TWAP) is a metric that is often used to optimize price by smoothing price volatility by taking an average market price over a period of time and can also be deployed to reduce market reaction to larger trades. *See e.g.* Amberdata Documentation, "Global TWAP" (available at https://docs.amberdata.io/docs/global-twap-2) for a definition.

[74] *See* CoW Swap Launches TWAP Orders, August 16, 2023, available at https://blog.cow.fi/cow-swap-launches-twap-orders-d5583135b472.

[75] *See* Jupiter Guides, How to Use Jupiter DCA for a more in depth explainer on functionality, available at https://station.jup.ag/guides/dca/how-to-dca

over a specified period of time to smooth out fluctuations in market price and open a position for an average market price" with a high degree of composability. The user can select the number of intervals, the total duration, the time between trades, whether the trades are equally weighted and can set price protections. Jupiter provides a dollar cost averaging solution to "enable users to automate the purchase or sale" at "regular intervals over a certain period of time."[76]

iii. Cost Saving Strategies. For the cost-savings use case, as another example of how user-initiated time delay implementations can benefit users, THORSwap streaming swaps are a mechanism the user may opt into to delay transaction activity (thus meeting the Proposal definition) but are intended to operate to give the user the choice and freedom to trade speed of execution for better price execution.[77] From a layman's perspective, they are intended to provide similar benefits to a trailing average pricing mechanism but over a more limited 24 hour period to smooth out price volatility. From a technical perspective, they operate on THORSwap "by allowing arb[itrage] to rebalance the pool between the streaming swaps."[78] This represents an improvement over traditional swaps. With basic swaps, you place the swap at a single moment in time thus requiring all liquidity needs of the swap need to be met at that one moment and arbitrage would work to restore liquidity after the transaction, streaming allows the swap to be fulfilled over a longer period, allowing arbitrage to correct and rebalance the price during the streaming swap. The user is able to control the timing and method of execution as follows:

- The **interval** variable in the stream allows the user to control the time between swaps; and
- The **quantity** variable in the stream allows the user to control the total amount of sub-swaps in the swap transaction to limit slippage per sub-swap while not expending capital to pay gas fees per sub-swap.

Streaming swaps also serve additional consumer protection functions as they have been shown to protect users from maximal extractable value (MEV)[79] attacks which could result in increased trading costs.[80] Implementing streaming swaps to break up larger transactions can disincentivize MEV attacks because there is an exponential decay in profit for MEV hunters due to hard costs as the swap gets smaller, making the sub-swaps that make up a streaming swap less attractive plays for MEV hunters.[81] As MEV is a practice that many crypto traders and owners seek to minimize or avoid, streaming swaps can be an addition to the existing user self-help tools and techniques that have been developed to protect users.[82] A number of these

[76] *Id*.
[77] *See* "Streaming Swaps" *https://docs.thorswap.finance/thorswap/thorswap/streaming-swaps* and "Introducing Streaming Swaps" explainer available at https://medium.com/thorchain/introducing-streaming-swaps-eff37f6150f3.
[78] *Id*.
[79] For more expanded and technical definitions of MEV and how it operates, *see* What is MEV? A Primer on Miner Extractable Value, https://blog.matcha.xyz/article/what-is-mev and Formalization of MEV, https://writings.flashbots.net/formalization-mev/. Though THORChain limits MEV by design, users have identified an absence of harmful MEV activity since the launch of streaming swaps. See "Tweet" by Rango Commander, @RangoCommander (January 21, 2024), https://x.com/RangoCommander/status/1732878516872503448 (observing that MEV phenomena like front running and sandwich attacks have not been seen in the THORChain system since the launch of time-delayed streaming swaps).
[80] Debates about the benefits versus drawbacks of MEV on blockchain transaction execution efficiency and fairness are beyond the scope of this comment. See description of that debate at Miner Extractable Value (MEV), https://ethereum.org/en/developers/docs/mev/.
[81] *See e.g.*, MEV Maximizing Strategies for Searchers, https://eigenphi.substack.com/p/mev-maximizing-strategies-for-searchers (describing strategies and frequency each strategy is deployed).
[82] For an early exploration of this issue, *see* MEV: A Scalability and Fairness Challenge in Blockchains, https://ar5iv.labs.arxiv.org/html/2212.0511, where the early solutions proposed were principally the time based and ordering based innovations that were principally developed and are described here.

tools rely on programmatic functions, including time delays.[83] These tools serve a valid consumer protection purpose, and bear similarity to other time-based trading execution delays implemented in traditional exchanges to serve the same purpose.[84]

iv. Emerging Use Cases. There are also countless use cases where user-initiated time delays could prove to be helpful - one multipurpose tool, CronCat,[85] offers decentralized scheduling for blockchain transactions and allows the user to set event-based automation so that tasks can react in the future when preset market conditions are hit or match criteria the user defines to execute. Additional use cases that would use user-initiated time delays range from estate-planning related functions where your own assets are transferred from self-custody to a Coinbase account in the event the wallet were dormant for a pre-designated period of time or a multi-sig function that boots a signer for inactivity or returns funds to a grantor due to lack of activity.

II. Addressing Crypto Industry Security Concerns Better Addresses National Security Concerns.

FinCEN is required by statute to consider "the effect of the action on national security and foreign policy". The Proposal, as drafted, has significant negative national security implications from constraining composability to labeling security best practices as having primarily criminal intent. We would think there is universal acknowledgement that security practices and standards need to be improved across the private and public sectors, not constrained.[86]

A. Inclusion of Security Best Practices.

In addition to the constraints on composability, we are particularly concerned about the impact of the Proposal on national security due to the inclusion of "security best practices." Rather than countering hacks and illicit actors, the Proposal will make people less safe and more vulnerable to such efforts. Hacks and exploits of vulnerabilities are endemic and not just a crypto-specific problem. As our world is increasingly digital, the U.S. needs to focus on developing better security and privacy tech across the board to combat illicit actors. However, the Proposal seeks to attach a pernicious intent to behaviors that generally make users ***safer*** when transacting on-chain, including:

---

[83] *See, e.g.*, Amirhossein Khajehpour and Hanzaleh Akbarinodehi and Mohammad Jahanara and Chen Feng, Mitigating MEV via Multiparty Delay Encryption, Cryptology ePrint Archive, Paper 2023/1612, 2023, available at, https://eprint.iacr.org/2023/1612 (proposing a mitigation tool through a multiparty delay encryption).

[84] From MEVBlock to Coincidences of Wants, there are a variety of self-help tools. See also the "speed bump" described in Michael Lewis, Flash Boys. *See also* https://www.sec.gov/files/rules/other/2016/34-78101.pdf. Blockwallet obscures the details of a transaction for a time before sending it directly to the miner rather than to the mempool. https://coincodex.com/article/13860/a-guide-to-mev-attacks-on-ethereum-and-how-to-prevent-them/. Batch auctions execute transactions at the same time regardless of the order in which they arrive, which is effectively a time adjustment for early orders. Timelock or threshold encryption mechanisms generated by projects like Ethermine and Flashbots hide transaction details from MEV extracting bots for a timeframe prior to execution. See https://bennyattar.substack.com/p/mev. The BSC network uses Sentry Nodes to minimize the public's interaction with nodes. *See* https://www.bnbchain.org/en/blog/mev-demystified-exploring-the-mev-landscape-in-the-bnb-chain-ecosystem. THORChain streaming swaps breaks larger swaps into multiple smaller sub-swaps executed over a period, a process that can serve to both optimize user fees and minimize MEV bots that may focus on otherwise larger swaps. https://docs.thorswap.finance/thorswap/thorswap/streaming-swaps.

[85] *See* CronCat Github https://github.com/CronCats ("CronCat provides a general purrpose [sic], fully autonomous network that enables scheduled function calls for blockchain contract execution").

[86] Though again, these issues are endemic and there are many actors that need to make this a focus - from cell phone providers not doing enough to combat sim swapping, to government agencies having significant issues with data breaches. See e.g., Ogier, Regulators' Data Breach Response Signals Challenges to Compliance with Its Own Rules, https://www.osler.com/en/blogs/risk/july-2023/regulators-data-breach-response-signals-challenges-to-compliance-with-its-own-rules. Within crypto, this is the subject of much debate in crypto with a number of security initiatives in development, including heightened efforts to coordinate self-policing efforts such as SEAL 911, "a collaborative initiative with white hat hackers, auditors and security leaders" formed in Q3 of 2023 see https://blockworks.co/news/defi-seal-911-white-hat-hackers-auditors. *See also infra* note 123.

i. **Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions.**[87] When transacting in digital assets, sending a test transaction is a well-known best practice to avoid potential risk of loss. Further, because the transactions are all on-chain, there is no anonymity or obfuscation gained from splitting up the transaction. Yet, the Proposal would erroneously label the splitting of a transaction into parts, which necessarily would include test transactions, as indicative of illicit behavior. Even if the language were narrower, as to capture the same sender splitting up payments to different wallets held by the same recipient. There are other legitimate reasons to break up transactions. More mundanely, a person may choose to store a portion of CVC on a hot wallet and send another portion to cold storage. This would also capture receiving a payment for work and then splitting it up among the workers. There are countless permutations of why and when this type of behavior may be warranted. For instance, someone may choose to keep cash in a savings account at one bank (or multiple banks in personal and joint accounts), cash in a money market account, and physical dollars does not raise regulatory red flags and neither should similar behavior, when conducted on chain.

ii. **Creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions.** Creating single-purpose or use wallets is a very standard procedure to reduce risks related to losses of seed phrases, theft, or just record-keeping purposes. It is considered a good practice because if your assets are stored in a single veritable honeypot where all your transaction history and total holdings are also viewable, you can more easily be the target of phishing and hacks. As described in a guide to choosing a wallet, when using hot wallets, "[u]sers can decide to create multiple hot wallets for different purposes. For instance, the best security practice is to create a new "burner wallet" for participating in NFT mints. Users may also create specific wallets for interfacing with DeFi protocols or gaming applications. This diversification protects against losing funds to a single hot wallet breach."[88]

Further, by declaring privacy-preserving features the object of suspicion, it produces a disincentive to continue to develop such features, which in turn exacerbates issues such as phishing attacks and results in greater user harm.

B. Constraining Composability Translates to a Negative Impact on User Safety.

As covered above, interoperability is necessary for the crypto ecosystem. There are many ways being explored to solve this, all of which involve a variety of tradeoffs in their design from a technical perspective, including impact on security, user experience, scalability, etc.[89] Even if the Proposal is pulled back such

[87] *See* Proposal at 8. Though much more broadly defined in the Proposal, " splitting a single transaction from sender to receiver into multiple, smaller transactions, in a manner similar to structuring, to make transactions blend in with other, unrelated transactions on the blockchain occurring at the same time so as to not stand out, thereby decreasing the probability of determining both intended persons for each unique transaction."

[88] Hot Wallets vs. Cold Wallets: What's the Difference?, Blockworks, https://blockworks.co/news/hot-wallets-cold-wallets; see also How to Manage Multiple Crypto Wallets: Best Practices, Request, https://www.request.finance/post/how-to-manage-multiple-crypto-wallets-best-practices ("[g]enerating multiple wallet addresses linked to the same seed phrase and private key is akin to having multiple bank accounts with identical login details. But this is not ideal, especially regarding resilience against hacks and implementing access controls."); Have Multiple Crypto Wallets: Why It's a Good Security Practice, MoonPay, https://www.moonpay.com/learn/cryptocurrency/have-multiple-crypto-wallets (discussing why having multiple wallets is a good security practice as well as wallet management practices); Wallet Security: Best Practices to Keep Your Crypto Safe, Hacken, https://hacken.io/discover/wallet-security/(includes having multiple wallets as a best practice as well as the use of burner wallets for airdrops in case of breach); An Introduction to Crypto Wallets and How to Keep Them Secure, QuickNode, https://www.quicknode.com/guides/web3-fundamentals-security/security/an-introduction-to-crypto-wallets-and-how-to-keep-them-secure (discussing security practices, including the use of multiple wallets).

[89] *See e.g.* Zetachain Part 1: A Competitive Landscape of Blockchain Bridges, January 4, 2024,

that it does not apply to all on-chain transactions, the Proposal may have the impact of chilling the remaining covered behaviors (outside of using mixers) and therefore pushing users toward other available options, some of which have been associated with increased security risks, thus further exposing users to hacks. For instance, as we have seen in 2022, North Korea has proved particularly adept at finding vulnerabilities in bridges. Thus, continuing to permit interchain transfers without forcing reliance on bridges means avoiding the problems associated with security risks of blockchain bridges that are a point of focus for FinCEN.

III. FinCEN is required to consider the Impact of the Proposals.

FinCEN is required to evaluate whether these new measures will impact national security, "create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organized or licensed in the United States"[90] or impact foreign policy, among other things. The Proposal fails to adequately weigh and consider these factors, which, together with its lack of factual basis correlating the purported risks to the activities covered, renders the rulemaking arbitrary and capricious in scope.

A. National Security.

Making arbitrary and overly broad rules as opposed to reasonable risk-based requirements will undermine the goal of regulating said behavior. Users will alter their behaviors to avoid impossible requirements; other efforts to comply or structure around these requirements would have the negative effects discussed above and divert resources away from addressing real risk. The U.S. would further cede this space and any innovations that come from it to less regulated jurisdictions as they will become the only places that the tech has a chance at surviving.

While FinCEN notes that "there is no reason to believe the required records and personal information contained therein would be subject to any greater risk of improper access, use, or exposure than any other record or report filed with a federal agency or maintained by a covered financial institution,"[91] this brings us no comfort. The state of data security is dire, including among government agencies and financial institutions. As most recently demonstrated by the Securities and Exchange Commission (SEC), which reportedly did not have two-factor authentication enabled on their Twitter account, government agency hacks and data honey pots have the potential to cause unparalleled value destruction. On January 9, 2024, the SEC's twitter was used to falsely announce ETF approvals[92] causing the second biggest wipeout of value in 2023.[93] By just analyzing price movement during the event, it resulted in a burn of over $50 billion

https://members.delphidigital.io/reports/zetachain-part-1-a-competitive-landscape-of-blockchain-bridges#stargate-de9d (discussing advances in infrastructure and composability stemming from the development of cross-chain message passing technology (with examples cited including ZetaChain, LayerZero, Axelar, IBC, Chainlink CCIP and others) and the deployment of omni-chain smart contracts).

[90] Proposal at 4.

[91] The Wilson Center, Blockchain: The World's Least Private Diary, https://www.wilsoncenter.org/article/blockchain-worlds-least-private-diary; see also Can Gurel, Everybody Needs *******, March 16, 2023 available at https://members.delphidigital.io/reports/everybody-needs/ (citing it is easy to see the need for privacy in crypto "given how constraining fully-transparent chains are. In most chains today, everyone can watch everyone. If you even make a single on-chain transfer to a friend, chances are, your friend will be able to not only see your entire transaction history, but also all your transactions in the future, forever.").

[92] Twitter Safety: 'Compromised' SEC Account Posted Fake Bitcoin ETF Tweet, Didn't Enable 2FA, https://decrypt.co/212251/twitter-safety-compromised-sec-account-posted-fake-bitcoin-etf-tweet-didnt-enable-2fa (citing that "the SEC's account did not have two-factor authentication enabled at the time of the hack, a security measure that SEC chair Gary Gensler had previously recommended as protection against identity theft and fraud").

[93] These statistics are pulled from chart analysis around price movement during the event but actual damage is hard to quantify outside of the event itself given this had follow on effects on the launch. The Tweet That Burned Over $50 Billion in Market Cap: A Deep Dive into the SEC Twitter Account Hack, https://medium.com/coinmonks/the-tweet-that-burned-over-50-billion-in-market-cap-a-deep-dive-into-the-sec-twitter-account-

in market capitalization[94] and destruction in value for 70,000 market participants via liquidations of $220 million over the course of the event.[95] Given the volume of records the Proposal would generate on everyday Americans and the sensitivity of the data contained, we urge FinCEN to take seriously the harm to national security and its citizens that will be caused by its insistence on propagating overinclusive and wide-sweeping reporting regimes. It is counterproductive and irresponsible for the government to continue to mandate the creation of honeypots of user data at covered financial institutions (and government agencies), which are in turn subject to increasing data breaches and phishing attacks, thus becoming the proximate cause of harm for consumers. Aggregating and pooling sensitive data should be avoided as it creates an unparalleled economic incentive for bad actors to increase and focus efforts to exploit vulnerabilities. It is especially harmful in crypto where the alternative is that your whole transaction history and net worth can be traced, including by criminals, leaving you more susceptible to personal and financial harm from everything from scams, fraud, identity theft, to physical threats and coercion.

B. Undue Burden.

As stated above, the Proposal seeks to attach a veil of suspicion to all uses and users of blockchain technology. The severity of the presumption created will result in denials of service and pose a threat to adoption, including through burdens that restrict access to off-ramps and covered institutions willing to serve as such off-ramps. Combined with the lack of regulatory justification here, these measures will impose undue burdens in a number of unprecedented ways. The Proposal is positioned as narrow in scope as it only applies "reporting obligations under this special measure … to covered financial institutions that directly engage with CVC transactions, such as a CVC exchange"[96] and covers behaviors that such institutions are largely already required to monitor[97] on and in this case, only in which the other party is non-U.S.[98] However, this is often impossible to determine and would drive compliance efforts to assume all transactions may hit this requirement if the data is unavailable. Under this Proposal, because mixing is equated to transacting on-chain,[99] the special measures require financial institutions to heighten their obligations beyond traditional AML procedure to report transactions taking place outside of the covered institution, including know-your-customer (KYC) compliance obligations to parties that are not their customers, thus imposing surveillance requirements to "collect unreliable data about people who have not opted into [a] service or signed up as [a] customer."[100] The requirement would likely entail collecting piles of incomplete and conflicting reporting of transaction information, and an unquantifiable amount of false red flags and SARs.[101] The sheer number of transactions that could fall under the Proposal for active users would be formidable to report, the data would be unavailable, and would instead result in denials of service

hack-34215b9c6752, see also SEC Twitter Hoax Sparks $2 Billion Bitcoin Transferred to Exchanges in Mayhem, https://cryptoslate.com/insights/sec-twitter-hoax-sparks-2b-bitcoin-transferred-to-exchanges-in-mayhem/.

[94] *Id*.

[95] SEC's Hacked Tweet on Bitcoin ETFs Causes Massive Trader Losses, Over $220M Liquidated, https://uk.investing.com/news/stock-market-news/secs-hacked-tweet-on-bitcoin-etfs-causes-massive-trader-losses-over-220m-liquidated-3293713

[96] Proposal at 33.

[97] Proposal at 34.

[98] Proposal at 6 ("transactions involving CVC mixing within or involving a jurisdiction outside the United States").

[99] From sending test transactions to using a company wallet that pooled crypto to receiving crypto from your employer via a streaming payroll, the Proposal is unprecedented in the scope of activities it covers.

[100] See similar arguments made in Square, Inc.'s Federal Comment Letter Regarding FinCEN's Proposed Rulemaking on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, January 4, 2021 (hereinafter "**Square 2021 Comment Letter**"), available at https://squareup.com/us/es/press/fincen-letter.

[101] Proposal at 29. FinCEN considered "issuing a rule pursuant to section 311 that would have been narrowly scoped to address terror finance involving Hamas and ISIS and/or North Korea-sponsored and -affiliated actors. However, FinCEN determined that such a narrow approach would be insufficient to address the relevant risks detailed elsewhere in this action. Given the nature and use of CVC mixing, covered financial institutions would typically have insufficient information to determine whether the CVC transaction was initiated [by] North Korean-affiliated actors." What is missing is how this Proposal adds to this goal.

and lack of access to off-ramps for every day users. It would take a significant policy interest to weigh against the level of burden created and FinCEN admits in the Proposal that the benefit is incremental, at best.

> "Although FinCEN recognizes much of the information that would be collected under this proposed rule is already provided to the most frequent reporters in the CVC ecosystem, imposing additional recordkeeping and reporting requirements is necessary to address the money laundering threat posed by CVC mixing because, at present, covered financial institutions do not regularly report when their customers send or receive CVC in transactions with indicia of CVC mixing."[102]

This reads as an attempt to chill on-chain activity and create denials of service because expanding the categories that would have an 'indicia' of CVC mixing to all on-chain activity creates an onerous surveillance regime that otherwise serves no legitimate policy purpose.[103] As we are all aware, the use of permissionless technology renders much of the information required uncollectable by such banks without the use and perpetuation of on-chain analytics and tracking software. While covered financial institutions are not required to diligence information not within their possession, they are required to adopt risk based approaches to fulfill their duties under the BSA.[104] Here, they are likely to flag self-custodied wallets and transactions not originating from U.S. CVC exchanges as they are required to report on transactions that a given team of banking personnel "knows, suspects, or has reason to suspect involves CVC mixing".

As we have described, given the definition, the bar for suspicious activity amounts to merely having transacted on-chain. ***Thus FinCEN is essentially mandating reporting of every customer CVC transaction to or from a covered institution except to the extent the counterparty is itself a covered financial institution.*** FinCEN's reporting rule would thus become a noisy and inaccurate signal. The reporting would predominantly cover lawful financial activity with no connection to illicit money laundering and the reporting data would be overwhelmed with false positives. Any potential incremental benefit is vastly outweighed by the cost, administrative burden (again an incomprehensible amount of noise and false alarms/SARs to any signal), and creates perverse incentives to avoid the rule, thus harming the underlying goal of aiding law enforcement efforts and national security interests. Further, it hinders U.S. competitiveness, seeking to fundamentally clash with the way the technology is designed to function instead of harnessing the elements of the technology that can aid law enforcement efforts.

Further, amidst all of the negative repercussions, there is nothing to suggest that this method improves upon current practices of flagging suspicious activity and tracing wallet addresses and on-chain activity. Covered financial institutions are already incredibly vigilant and overinclusive in diligence and derisking activities. Current surveillance methods and technology have been proven incredibly effective and are much more immediate than sorting through countless reports containing information (if known) about everyday transactions. Further, citing a rationale of using this reporting to identify the types of mixers used and "assist

---

[102] Proposal at 34.

[103] This is all but admitted in the Proposal, page 27. "[C]overed financial institutions already possess customer information and can identify when their customers engage in a covered transaction. This proposed rule would compel covered financial institutions to attribute a covered transaction to the involved customer(s) and report this information to FinCEN."

[104] *See* Proposal at 33-34 for a description of existing obligations and under the new proposed rule, these same institutions must collect, maintain records of, and report to FinCEN within 30 calendar days of initial detection of a covered transaction. These institutions include not just banks, exchanges and payment processors, but also covered institutions include, among other things, broker dealers, FCMs and mutual funds.

in understanding trends of mixing activity as well as aid in understanding the quantity of CVC mixers in the CVC ecosystem" is nonsensical as there are many more productive and direct ways to do so with significantly less negative externalities. Again, the activity is all on-chain and tracing and analytics companies already assist law enforcement with surveillance and remedial efforts with a high degree of success.

Far from ensuring that "the purposes of section 311 are fulfilled" by guarding against money laundering and crime, this creates insurmountable record keeping and verification requirements by surveilling everyday legitimate behaviors and transactions – this could capture countless everyday transactions per year for active users in the space, constrains composability and chills security and privacy technological innovations – all at the direct harm to users. The existing reporting regime has been analogized to reporting obligations so overinclusive that they require finding needles in haystacks – we are now requiring reporting on every piece of hay. As we have seen continuously, efforts like these produce noise rather than signal with the primary result being chilling effects on banking relationships with financial institutions 'derisking'[105] by increasingly opting out of engaging with users of this technology rather than trying to sort through compliance in an unwinnable battle. As Treasury has acknowledged in a 2023 report, derisking is harmful to the Treasury's goals of protecting against illicit finance. "De-risking can increase the use of financial services that exist outside of that regulated financial system, undermining the purposes of the BSA by making it harder to detect and deter illicit finance. The marginalization of certain categories of customers through de-risking also raises the specter of sanctions evasion. Increased reliance on unregistered financial mechanisms by customers excluded from the regulated financial system can create a potential profit center for criminals. De-risking could also lead to an erosion of the centrality of the United States in the international financial system."[106]

C. Competitive Disadvantages.

The Proposal introduces artificial constraints and arbitrary frictions that will cause competitive disadvantages. The Proposal itself states that an expected outcome is "that the relative attractiveness of engaging with CVC mixers or the number of those who avail themselves of CVC mixing services might be affected."[107] Meaning that a goal of the Proposal, given the breadth of the definition of CVC mixing, is to choke off ramps and harm mainstream adoption. This statement belies the true intent of this Proposal, which is to conduct an Operation Chokepoint 3.0[108] and effect another denial of service to users and developers in this space and be the proximate cause of "significant adverse systemic impact…on legitimate business activities involving the particular… class of transactions".[109]

Given the weight of the unprecedented action here, it is inevitable that covered institutions would seek to avoid engaging with these types of transactions and users to avoid compliance burden potential liabilities –

[105] *See* https://www.wsj.com/articles/the-unintended-consequence-of-closing-high-risk-accounts-1459589407 (explaining why this derisking behavior is counterintuitive to the goals of the BSA regime); *see also* https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf ("**2023 AMLA Report**")

[106] *See* 2023 AMLA Report *supra* note 105, at 5.

[107] Proposal at 53.

[108] Again, the intent is made clear here when FinCEN assesses the risk to the payment system and legitimate business activities involving CVC, it concludes the implementation would have minimal impact because "direct connections between CVC and systemically important financial institutions and core financial markets are limited at present." and the CVC ecosystem lacks connections to mainstream markets – meaning that FinCEN has entirely skipped the requirement to assess the impact to the CVC ecosystem and intends the rulemaking to act as a tool to further contain the CVC ecosystem and keep it separate from traditional markets rather than having any legitimate policy purpose.

[109] Proposal at 4 (describing a factor that is required to be considered).

those who are not yet engaged in CVC transactions are likely to refrain either directly denying service or under cover from prudential regulators citing safety and soundness. Those who are will be subject to these heightened requirements - thus placing more burden on these institutions than is required of traditional institutions that deal in cash.[110] We are once again compelled to remind regulators that cash is more of a heightened threat than CVC.[111] However, the harm will not just be to the intended target here, adoption of the technology will be stifled in the broader U.S. market as U.S. institutions are denied the ability to develop upon the tech to leverage the strengths of using innovations that utilize smart contract features like time based features, continuous swaps, etc. Congress recently held a hearing on January 18, 2024 entitled, "National Security Challenges: Outpacing China in Emerging Technology" where a witness stated that "whichever nation dominates the technology revolution— particularly in emerging technology areas … will likely also win the larger geopolitical competition."[112] This administration, through its deep animosity towards technology is all but ceding that battle to the detriment of America's competitive future. As we have seen consistently, the U.S. has been steadily losing developer share in crypto since 2018 and now only 26% of crypto developers are based in the U.S.[113] The Proposal now seeks to hardwire the politically driven determination that crypto is an "undesirable" industry and will further deter crypto development in the U.S., not just to the detriment of the industry itself, but will prevent research and development efforts that could have wide reaching benefits and applications and lead to competitive advantages internationally.[114]

Respectfully, we would suggest a more productive path for all is to focus less on chasing the innocent and focusing on the guilty. Undoubtedly, this rulemaking will keep driving nails into the coffin to ensure crypto-native development is pushed further offshore, covered institutions will seek to avoid the compliance costs of interactions that could lead to heightened obligations,[115] others may discontinue lines of business and

[110] "The United Nations Office on Drugs and Crime estimates that as much as $2 trillion is illegally laundered around the world each year — while law enforcement reportedly catches less than 1% of that. As much as $300 billion in illicit funds make their way through the U.S. financial system in a given year, according to the Treasury Department….For bankers, the sheer volume of information that must be filed under current standards can be overwhelming to comprehend — more than 15 million reports per year on cash transactions over $10,000 and suspicious activities." In 2017, a study "of 19 major banks found that they produced 640,000 suspicious activity reports and 5.2 million currency transaction reports in 2017, based on 16 million alerts. But law enforcement agencies followed up on only 4% of the SARs and less than 0.5% of the CTRs." FinCEN now seeks to introduce a rulemaking that ratchets up the volume and scope of the reporting that already "created mountains, literally, warehouses full of mainly innocuous transactions" for banks. *See* Is there a Better Way to Fight Money Laundering, American Banker, available at https://www.americanbanker.com/news/is-there-a-better-way-to-fight-money-laundering.

[111] Given the number of recent rulemakings that have ignored this fact, these arguments have been well-covered in comment letters. *See, e.g*., Square 2021 Comment Letter *supra* note 100 (citing "[t]he incongruity between the treatment of cash and cryptocurrency under FinCEN's Proposal will inhibit adoption of cryptocurrency and invade the privacy of individuals. Yet the rule fails to explain the difference in risk. As such, this low threshold and its extension of KYC obligations beyond customer relationships is arbitrary and unjustified.").

[112] Statement for the Record of Jamil N. Jaffer on National Security Challenges: Outpacing China in Emerging Technology, before the United States Senate Committee on Banking, Housing, and Urban Affairs, January 18, 2024, available at https://www.banking.senate.gov/imo/media/doc/jaffer_testimony.pdf, at 4. Also citing in his testimony the need to not only play defense but to continue to innovate "to ensure the U.S. is able to effectively compete with China. "[T]he government should provide significant tax and other economic incentive to startups, as well as other companies that can rapidly and massively scale up (therefore effectively compete with Chinese national champions)—and remove existing regulatory and other barriers—for increased private basic and applied R&D investment in critical emerging technology areas like: (1) high-performance and accelerated computing; (2) quantum technology; (3) cloud and edge computing capabilities, particularly for the warfighter; (4) AI/ML capabilities, including generative AI, as well as capabilities to enhance the trust, safety, and security of AI-enabled systems; (5) design and production, in the United States and allied nations, of both commodity and bleeding-edge semiconductors, particularly for artificial intelligence and other critical applications; (6) production and processing, in the United States and allied nations, of critical minerals necessary for national security and technology applications; and (7) enhanced cybersecurity efforts and protection of intellectual property." *Id.* at 9.

[113] *See* Electric Capital 2023 Developer Report, https://www.developerreport.com/developer-report (with the executive summary citing a 14% decline over that time span); *see also Id*. at 174 - 177.

[114] For instance, in crypto, more frictionless transfers between chains eliminates the pathologies seen in the Forex markets. Forex analogy in crypto world transactions between different crypto communities is becoming much easier via atomic swaps or avalanche subnets or other new interchain tech, it is then easier to use crypto for multiple purposes (money & utility) and fulfill broader use cases and market needs, including research and development efforts that could improve market infrastructure from automating trade execution to improving settlement The counter argument is that covered institutions would develop this themselves and be exempt. See discussion in "Competitive Disadvantages".

[115] Harvey Gee, Last Call for the Third-Party Doctrine In the Age After Carpenter?, 26 B.U. J. SCI & TECH. L. 286, 288 (2020).

still others will likely be chilled from entering the space, understanding the technology or participating given the presumption of illicit activity attached to these activities.

D. Foreign Policy and Commerce; Existence of Similar Regulatory Treatment.

From a foreign policy and commerce standpoint, the Proposal will raise costs, reduce competitiveness, and potentially lead to jurisdictional conflicts, particularly concerning privacy and data protection laws. The extensive increase in personal data collection, including data related to third-party non-customers, coupled with record-keeping requirements pertaining to transactions "within or involving a jurisdiction outside the United States," is likely to clash with regulations like the GDPR.[116] European courts have expressed concerns about the large-scale retention of sensitive information by U.S. companies, and this expanded data collection could further strain the ability of U.S. covered institutions to serve these markets competitively.

FinCEN is also required to examine "whether similar action has been or is being taken by other nations or multilateral groups."[117] FinCEN admits that "FinCEN is not aware of any other nation or multilateral group that has imposed, or is currently imposing, similar recordkeeping and reporting requirements relating to transactions involving CVC mixing."[118] Instead, the Proposal relies on a limited set of examples of jurisdictions calling for "appropriate" regulation for CVC mixing, defined with a narrow scope to cover mixing services with an intent to obfuscate[119] and such efforts are in all cases presumed to address when such obfuscation is in furtherance of a crime rather than the expansive definition being advanced in the Proposal.

******

We appreciate the opportunity to comment on the Proposal. While we agree the stated goals of the Proposal are important ones to meet, we believe the current Proposal falls short of advancing or achieving them. Requiring the reporting of every customer CVC transaction to or from a covered institution, without accompanying robust risk and economic analysis, is arbitrary and capricious - it lacks fairness and a rational purpose. As U.S. citizens who hope to see innovation take place at home and for the basic economic future of our country, we feel strongly that rulemaking in this area should not purely seek to increase state influence regardless of cost.[120] In this case, significant unassessed costs exist, while FinCEN has not identified tangible benefits from the rulemaking, including the ability to meaningfully process these reports. There are also more immediate, productive and direct means of addressing FinCEN's concerns without the incredible collateral damage the Proposal would introduce and they include the continued development of security measures, with privacy tech and the further development of cryptography being key tools that we must continue to develop to thwart bad actors.

---

[116] Proposal at 76; see also https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9090724&fileOId=9090725

[117] Proposal at 4.

[118] Proposal at 25.

[119] *See, e.g*. this cited analysis from Australia, which states that "[c]riminals can take advantage of conversion services, such as mixers" PREVENTING THE CRIMINAL ABUSE OF DIGITAL CURRENCIES: FINANCIAL CRIME GUIDE, April 2022, available at https://www.austrac.gov.au/sites/default/files/2022-04/AUSTRAC_FCG_PreventingCriminalAbuseOfDigitalCurrencies_FINAL.pdf.

[120] Economic theory predicts that economic growth is dependent on "regulatory policies that promote competitive markets, secure property rights, and intervene to correct market failures rather than to increase state influence," U.S. Office of Management and Budget, 2006 Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/assets/OMB/inforeg/2006_cb/2006_cb_final_report.pdf (U.S. OMBD citing economic theory) (emphasis added).

In our increasingly digital world, modern surveillance technology has and will continue to offer law enforcement the unmatched ability to detect, trace and collect evidence on the activities of bad actors, with less impact on privacy than the proposed rulemaking. In a world of surveillance that more than meets these needs, the third party doctrine does not need to continue to be stretched and weaponized for the government to liberally glean the most intimate details about users of technology" by making every on-chain act reportable and chilling the use of privacy preserving technology. FinCEN itself admits that on-chain transactions are public and traceable[121] and 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" but then attempts to police everyday mundane behaviors that occur in unfathomably large volumes on permissionless networks and are undertaken with legitimate business (and consumer) applications. These are not just unduly burdensome and counterproductive requirements, they represent an extreme and concerning overreach. So while we believe that existing surveillance technology better addresses law enforcement surveillance needs, we also believe that efforts to improve security and protect users[122] are essential to the end goal of the Proposal and to the U.S. protecting its interests in an increasingly digital world. These initiatives should be aggressively advanced – not be arbitrarily constrained with the result of making everyone less safe.

In the event FinCEN were to move forward with a rulemaking to cover "mixing" activity on its face, which seems to be the underlying concern, FinCEN should be narrow and surgical – carefully weighing the incremental benefit of such rulemaking against its ability to continue to use the many additional tools at the disposal of U.S. regulators, including (i) enforcement against bad actors, (ii) its ability to provide guidance in the market on best practices to address national security concerns and (iii) actively participate in ongoing efforts to increase prophylactic measures such as security best practices and remedial measures such as on-chain analytics and wallet tracing.[123]

---

[121] Proposal at 7 (stating "[t]he public nature of most CVC blockchains, which provide a permanent, recorded history of all previous transactions, make it possible to know someone's entire financial history on the blockchain").

[122] *See* What Should Crypto do About Consumer Fraud, https://members.delphidigital.io/feed/what-should-crypto-do-about-consumer-fraud (stating that efforts to increase security practices and help protect users from bad actors are paramount).

[123] For a sampling of these activities, (i) security researchers play an important role in the space and their work, together with a large academic involvement with several universities, including Cornell, Stanford and ETH Zurich among other prominent institutions, do important research and development on security practices (see, e.g., IC3 https://www.initc3.org/about.html); (ii) organizations and initiatives such as DeFiSafety, which is one of many organizations that specializes in technical risk analysis to evaluate blockchain protocol quality and provide safety ratings (see https://www.defisafety.com/about), there are broader organizations also working on best practices from the Security Alliance (see e.g. https://securityalliance.notion.site/Twitter-Security-Self-Audit-8fdb80d93a144dbab0f0cc4ff59c2131) ands
L2beat (providing reports and services that are an "audit" in that it's a checklist of quantitative measurements where a percentage score of adherence to an encoded set of best practices and those best practices are scored according to an open source rubric); (iii) there are hundreds of active code review organizations and projects invoking good security practices undergo a host of security checks from basic code review, formal verification, economic modeling, agent-based simulations, among many other tools and security auditors often release findings that may benefit the open source community (see e.g. https://research.kudelskisecurity.com/2023/03/23/multiple-cves-in-threshold-cryptography-implementations/) (iv) many organizations, including code audit organizations, actively fund security tooling and initiatives, such as Open Zeppelin (see https://contracts.openzeppelin.com/security as well as resources from Trail of Bits, Chainsecurity; (iv) the open source community releases learnings such as the many open source guides on solidity best practices (see, e.g. https://github.com/transmissions11/solcurity, https://github.com/nascentxyz/simple-security-toolkit and
https://github.com/ComposableSecurity/SCSVS/tree/master, https://github.com/crytic/building-secure-contracts, (v) on a design level, it is demonstrative is that the industry spends many multiples on security auditing services than other industries and is actively pushing the envelope very far on formal verification technology, incorporating this deeply into design practices, (vi) security researchers also engage in investigations and whitehat initiatives, undertake forensics and participate in active response teams in the wake of a hack, including ETHSecurity Community members and Seal 911 members (see ttps://gist.github.com/samczsun/366b853a54391a97ab13cd2e3ca2d7c9); (vii) from a remedial perspective, a host of tools and forensics have been developed and can be deployed to identify the bad actor and facilitate the return of funds from on visualizers, chain analytics (i.e. Glassnode, Dune, Nansen, DefiLlama, Etherscan, Token Terminal, DeBank) to de-mixing tools such as amlbot.com/reclaim-crypto. Researchers, projects and the broader open source community often also help in post-mortem exercises to investigate the root cause of a vulnerability so that others can prevent similar exploits (see, e.g., https://twitter.com/pcaversaccio; https://github.com/pcaversaccio/reentrancy-attacks).