January 22, 2024

BY ELECTRONIC SUBMISSION

Andrea Gacki
Director
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183
Attn: FINCEN–2023–0016

Re: *RIN 1506-AB64: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*

Dear Director Gacki:

Andreessen Horowitz ("a16z") appreciates the opportunity to respond to FinCEN's proposed special measure regarding convertible virtual currency mixing as a class of transactions of primary money laundering concern.[1] We welcome an opportunity to meet with FinCEN staff and answer any questions that the agency may have and to discuss our comments below in more detail.

A16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on bio and healthcare, consumer, crypto, enterprise, fintech, and games. A16z currently has more than $35 billion in committed capital under management across multiple funds, with more than $7.6 billion in crypto funds. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch Internet businesses. Our funds typically have a 10-year time horizon, as we take a long-term view of our investments, and we do not speculate in short-term crypto-asset price fluctuations.

At a16z, we believe we need an Internet that can foster competition and mitigate the dominance of large technology companies, unlock opportunities in the innovation economy, and enable people to take control of their digital information. The solution is web3—the third generation of the Internet—a group of technologies that encompasses blockchains, digital assets, decentralized applications and finance, and decentralized autonomous organizations. Together, these tools enable new forms of human collaboration that can help communities make better collective decisions about critical issues, such as how networks will evolve and how economic benefits will be distributed. We are optimistic about the potential of web3 to restore trust in institutions and expand access to opportunity.

[1] *See Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, 88 Fed. Reg. 72,701 (Oct. 23, 2023).

I. Summary

One of the most difficult questions that our regulators and legislators face is how to strike the right balance between Americans' valid privacy interests and the country's national security needs. Without a doubt, our nation faces grave national security challenges, and absent the safety and security that the government provides, our companies could not advance technologies that benefit all Americans. However, we believe that FinCEN's proposed special measure and reporting requirements has, perhaps unintentionally, tipped the scales entirely in favor of America's national security objectives, while failing to appropriately accommodate Americans' privacy concerns. As explained in the sections that follow, we respectfully suggest that the options facing FinCEN are not zero-sum, and that more can be done to support, or at a minimum not inhibit, emerging privacy technologies.

First, the proposal would be bad for privacy, cripple innovation, and make law enforcement more difficult. This broad targeting of technologies that are necessary for law-abiding persons and businesses to use digital assets without public exposure prevents promising developments needed for blockchains to become widely adopted and successful. Worse, the proposal would move the center of gravity for blockchain activities away from highly regulated financial institutions and away from America, thereby reducing law enforcement's ability to collect evidence, recover illicit assets, and effectively oversee digital asset activities in the long run.

Second, the proposal is overbroad along multiple dimensions. The six categories of "mixing" defined by the proposal reach too much lawful activity. Although the proposal focuses on the illicit conduct that its six categories cover, their terms are broad and appear to also reach routine and innocuous transactions. On our reading, they could reach basic practices like Unspent Transaction Output (UTXO)[2] transactions on certain blockchains, ordinary tools like smart contracts, as well as privacy-preserving technologies designed to protect digital asset users.

Third, the proposal's foreign-nexus requirement exacerbates these problems. Most blockchain transactions include indirect connections to foreigners and the location of users is often impossible to discern. And the proposal's exposure threshold, which requires financial institutions to monitor and report transactions in the past and future to which they are not parties, exponentially increases the overbreadth and associated costs of the proposal. In effect, the proposal could taint many lawful blockchain activities with an inaccurate money-laundering label, making dealing with them prohibitively burdensome for reporting entities, and causing the proposal to operate as a de facto ban.

We also believe that the proposal raises several legal questions that could present unnecessary litigation risk.

[2] An Unspent Transaction Output or UTXO is an unused or leftover cryptocurrency in a transaction. Ledger Academy, *Unspent Transaction Output UTXO meaning* (July 23, 2023), perma.cc/Q2AQ-DQU2.

We recommend a narrower approach. Instead of identifying broad generic categories of activities, we recommend identifying discrete mixing entities or technologies used primarily for illicit activities, covering only those transactions to which financial institutions are parties or intermediaries, and exempting privacy-preserving technologies that use protective measures designed to prevent their use by illicit actors. We also recommend that FinCEN not treat transactions as presumptively foreign and that reliance on Suspicious Activity Reports designed to more effectively capture blockchain data and other more precise mechanisms would more effectively accomplish its important goals. Last, we urge FinCEN to submit a revised proposal to a new comment period in light of the substantial uncertainty surrounding its possible scope and implications.

II. The special measure undermines law enforcement, privacy, and innovation.

We begin with a policy discussion of why the special measure as proposed will erode and counteract important interests in law enforcement, privacy, and innovation.

A. Law enforcement

A16z strongly agrees with FinCEN's goal of "defend[ing] the United States financial system from money laundering and terrorist financing risks."[3] These threats are serious, and we agree that FinCEN must have the authority to gather credible evidence of these risks before they escalate. But labeling broad swaths of the blockchain ecosystem as of "primary money laundering concern" will not be an effective means toward that end, and for the reasons described below, it may even be affirmatively counterproductive.

First, the proposal could lead regulated financial institutions to cease engaging in blockchain-based transactions or doing business with customers who use digital assets. This is the exact opposite state of affairs that regulations should incentivize. At this time, a significant portion of digital asset activity in the United States runs through regulated exchanges and financial institutions that serve as on- and off-ramps for users to exchange their digital assets for fiat and vice versa.[4] It is precisely these financial intermediaries that have deep experience in money laundering, consumer protection, and other laws. Moreover, law enforcement depends upon financial intermediaries for crucial attribution evidence and expedient asset recovery. Existing regulatory and legal frameworks allow law enforcement to readily obtain information about suspected criminal activity involving digital assets and to effectively implement sanctions and other limitations through those financial institutions.[5] A more optimal regulatory outcome would, therefore, be to encourage more access to the traditional financial system, not less, but in a safe and regulated manner.

Second, the proposal will move the center of gravity for blockchain activity away from the United States and into foreign jurisdictions. Because blockchains are a decentralized, global, and open technology, they will always exist somewhere, and can

[3] *Id.* at 72,701.
[4] *See, e.g.*, *North America Leads World in Crypto Usage Despite Ongoing Regulatory Questions, While Stablecoin Activity Shifts Away from U.S. Services*, Chainalysis (Oct. 23, 2023), perma.cc/R4VF-P6YH.
[5] *See, e.g.*, *United States v. Coinbase, Inc.*, 17-cv-01431, 2017 WL 5890052 (N.D. Cal. Nov. 28, 2017).

migrate to jurisdictions with less restrictive laws and regulations. Moreover, state actors from adversarial regimes such as DPRK, as identified in the proposal, will still have access to digital assets and mixing tools, but law enforcement would have less visibility into activity without touchpoints in the United States. Currently, that access is mitigated because the United States is a major global hub of blockchain companies and activities, so appropriately tailored American government policies can curb excesses and dangers in blockchain technology. Absent that, blockchain technology is likely to develop beyond our reach, making investigative and regulatory efforts much more difficult.

Third, if the proposal does not effectively cause financial institutions to cease engaging in digital asset activity, it will result in an overwhelming number of reports that will make effective supervision of the blockchain ecosystem impossible. The breadth of the proposal—in terms of the six categories, its effective coverage of all domestic transactions, and its indirect-exposure aspect—reaches an unprecedented number of transactions. Every time a money transmitter converts cryptocurrency that was sent using the basic UTXO aggregator function, it will send a report. Every time an exchange sees a customer using smart contracts to time payments, it will send a report. And every time a financial institution has a customer who stakes, it will send a report. These covered transactions would happen by the millions. The associated reports will flood FinCEN with more paperwork than it can feasibly make sense of. It will render it difficult for FinCEN, and the law enforcement investigators the reports are designed to benefit, to find the small number of reports and narratives that identify illicit activity. In other words, criminals will be better off than before because the reports about their activity will be buried in the crowd of millions of reports about lawful activity.

B. Privacy

The proposal tells one side of the story of privacy-preserving technologies—that they are being used by criminals. But we believe there is another important side to that story, which underscores why the special measure should be rethought.

As the proposal recognizes, privacy-preserving technologies are crucial to law-abiding users: "The 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. Anonymity enhancing tools, including 'mixers,' are used to avoid this."[6] In other words, due to the nature of public ledger technology, law-abiding users *need* privacy-preserving technology. Without privacy-preserving technology, ordinary digital asset transactions can create acute vulnerabilities. Consider, for example, a mom-and-pop shop that accepts payment in digital assets from its customers. Without privacy-preserving technology, the store's cashiers could access their customer's financial activity information—for example, where that customer shopped yesterday or the customer's total digital asset holdings on the respective blockchain network used for the transaction. Likewise, an employer that pays its employees in digital assets can access all of the employees' transactions, donations, and holdings if the employees do not have access to

[6] 88 Fed. Reg. at 72,702.

privacy-preserving technology. Businesses will also have access to their competitors' blockchain-based transactional data, which could result in an economically skewed market.

Privacy-preserving technology is also essential to prevent other harms. It allows people to make sensitive transactions, such as paying for healthcare services, in confidence.[7] It allows them to exercise their constitutionally protected associational rights.[8] It allows them to undertake activities that could draw retaliation from authoritarian regimes or foreign terrorists, such as donations to Ukrainians to fight against Russian invasion.[9] And it allows large holders of digital assets to keep their families safe by preventing others from discovering their holdings.[10] All of these activities are lawful, but all of them depend on privacy-preserving technologies like those targeted by the special measure.[11] Otherwise, those users might have their every transaction and every asset exposed to the rest of the world for all time.

In fact, there are significant national security benefits to privacy-preserving technology. As FinCEN is aware, on most public blockchains, all of a person's digital assets and transactions are available for anyone to see, including adversaries of the United States, like DPRK, China, Iran and Russia, as well as non-state actor cybercriminals. While a person transacting on a public blockchain does have some degree of privacy protection because of the pseudonymity of wallet addresses, data analytics have become increasingly good at surmounting pseudonymity.[12] Accordingly, without the privacy afforded by enhanced layer-1 blockchains, mixing services, or other technologies, our adversaries could use surveillance networks to monitor our citizens through their blockchain transactions. Privacy-preserving technologies are, therefore, a crucial line of defense against such surveillance.[13] But, the important takeaway is that not all "mixing," as FinCEN broadly defines such activity, either "mixes" by function, as described in Section III below, or is intended to launder, confuse, or obfuscate.

We believe that FinCEN can accomplish its national security goals without overly intruding on Americans' privacy. Few things have a higher place in American legal history than the "cherished privacy of law-abiding citizens."[14] In the words of former Supreme Court Justice William O. Douglas, "[t]he right to be let alone is indeed the beginning of all

---

[7] *See* Tuminelli & Whitehouse-Levine, *When Did Privacy Become a Bad Word?,* CoinDesk (Aug. 25, 2023), perma.cc/26PB-ZREX

[8] *See* O'Sullivan, *What are mixers and "privacy coins"?,* Coin Center (July 7, 2020), perma.cc/J4G3-W9TQ.

[9] *See Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, CISA (May 9, 2022), perma.cc/C5TN-QL62.

[10] Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, N.Y. Times (Feb. 18, 2018), perma.cc/3KCU-3ELC.

[11] *See* Weinstein, *AI and Blockchain Analytics: The Urgent Need for Crypto Privacy Tools*, Forbes (Apr. 7, 2023), perma.cc/M65D-4ER2.

[12] *See* Justin Sherman, *Big Data May Not Know Your Name. But It Knows Everything Else*, Wired (Dec. 19, 2021), perma.cc/6LY7-ARPU.

[13] *See* Timm, *The Importance of Responsible Privacy in Digital Assets*, Iron Fish (Oct. 6, 2022), perma.cc/FQK3-KP9E.

[14] *United States v. United States District Court*, 407 U.S. 297, 312 (1972).

freedom."[15] "Privacy of personal matters is an interest in and of itself;"[16] it is protected by multiple provisions in our constitution;[17] it is protected by common law;[18] and it is guaranteed by numerous federal and state statutes.[19] As we will discuss further in sections that follow, we strongly urge FinCEN to narrow or rethink the proposed special measure to more appropriately balance Americans' development of and access to emerging and privacy-preserving technologies with necessary national security objectives.

C. Innovation

A16z shares FinCEN's interest in promoting and preserving "innovation and advances in digital distributed ledger technology."[20] We agree with the current Presidential administration's commitment to "foster[ing] responsible digital asset innovation," in keeping with the long-standing "U.S. government … role in priming responsible private-sector innovation" through "sponsor[ing] cutting-edge research" and "help[ing] firms compete globally."[21] We also appreciate Treasury's recognition that "responsible innovation has been a motto for [the] Department" and that "[i]nnovation" is "a ladder, to help more people climb to a higher quality of life."[22]

Unfortunately, the proposal would stifle innovation and advances in blockchain technology. We believe that privacy-preserving technologies, which this proposal targets, go hand-in-hand with legitimate and innovative uses of digital assets. Privacy-preserving technologies are necessary for blockchains and digital assets to thrive. In other words, the proposal's premise that privacy-preserving technologies "undermin[e] the legitimate and innovative uses of CVC" is mistaken. While illicit conduct can thrive in a wide range of environments, many lawful activities require the security and confidentiality that only privacy-preserving technologies can provide.

The history of the Internet provides a close analogy.[23] In the early days of the Internet, many believed that because of its anonymized, decentralized nature, it would be used primarily for crime and lawlessness.[24] Many held the view that the "internet cannot be regulated."[25] At the same time, law-abiding businesses and citizens did not rely on the Internet because their activities were too exposed and insecure without strong privacy

---

[15] *Pub. Utilities Comm'n of D.C. v. Pollak*, 343 U.S. 451, 467 (1952) (Douglas, J., dissenting).
[16] *Roberts v. Austin*, 632 F.2d 1202, 1214 (5th Cir. 1981).
[17] *E.g.*, *Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373 (2021); *Katz v. United States*, 389 U.S. 347 (1967); *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[18] Brandeis & Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[19] *E.g.*, Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3423 (protecting the confidentiality of personal financial records).
[20] 88 Fed. Reg. at 72,702.
[21] *Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, The White House (Sept. 16, 2022), perma.cc/8CQA-YRMB.
[22] *U.S. Treasury Department Holds Financial Sector Innovation Policy Roundtable*, Dep't of Treasury (Feb. 10, 2021), perma.cc/D3LU-UL6Z.
[23] *See A Letter to the White House: Aleo's Response to the OSTP*, Aleo (Mar. 3, 2023), perma.cc/GSD3-5PLN.
[24] Goldsmith & Wu, *Who Controls the Internet* xii (2006) ("In the 1990s, many believed that nations could not control the local effects of unwanted Internet communications that originated outside their borders, and thus could not enforce national laws related to speech, crime, copyright, and much more").
[25] Goldsmith & Wu, *Who Controls the Internet* 3 (2006) (quoting MIT Media Lab co-founder).

guarantees. Then, a wave of privacy-preserving technologies, including some of the same encryption methods underlying modern blockchain technology, were introduced.[26] Instead of making the Internet home to *more* criminal activities, these technologies made it finally welcoming to lawful and institutional uses. Privacy-preserving technologies allow confidential information to be transmitted over the Internet securely and privately. As a result, hundreds of millions of Americans, as well as every major corporation and governmental agency, adopted the Internet for their most confidential activities, including their bank accounts, medical records, and personal communications. Thus, by the numbers, criminality became a smaller proportion of online activity. Today, privacy coexists with law-enforcement tools that allow meaningful investigation of activity on the Internet, including through technologies that have developed in tandem with the Internet and allow law enforcement to monitor and prohibit illegal activity without eliminating a basic level of privacy. If these privacy-preserving technologies had been stopped in their tracks, the Internet would have remained a wild west for people willing to take their chances with unprotected information. We would have never seen the ubiquitous lawful and institutional uses familiar today. This proposal as currently written risks killing the dream of an open network that fosters creativity and entrepreneurship.

Blockchains and digital assets can help launch these concepts of democratizing ownership and a more secure and trusted Internet to the next level.[27] Blockchain and decentralized technology allows for innovative new forms of ownership and control of the next generation of digital services. Like the Internet, it is creating homegrown American companies and jobs. And as they have since the first bitcoin transactions rolled out, law enforcement will continue to develop effective methods to prevent illegal uses of the technology without eliminating basic privacy for everyone else. For this reason, we respectfully encourage FinCEN to exercise caution with special measures that may unintentionally disrupt positive innovations and developments in the blockchain ecosystem.

III. The special measure is overbroad and unclear along multiple dimensions.

A. The six categories of "mixing" encompass largely lawful activity.

As drafted, the proposal applies to any transaction that a financial institution suspects, has reason to suspect, or knows "involves CVC mixing."[28] It defines "CVC mixing" to include facilitating transactions in a manner that "obfuscates" the source, destination, or amount of crypto being transmitted,[29] and classifies all transactions within six broad categories as of "primary money laundering concern."[30] We discuss the obfuscating clause and each of the six categories below.

[26] *See, e.g.*, Singh, *The Code Book* 293-317 (1999).
[27] *See* Hall et al., *A few of the things we're excited about in crypto* (2024), a16z crypto, perma.cc/88AU-ENCQ.
[28] 88 Fed. Reg. at 72,722.
[29] *Id.*
[30] *Id*. at 72,704.

As a threshold matter, it is unclear whether the obfuscation clause modifies the six categories. If it does not, then the categories are deemed "mixing" even without an obfuscation element. In that case, the six categories are wholly unworkable. If it does, then the categories are deemed "mixing" only when the activity satisfies some separate standard of obfuscation. In that case, the categories remain overbroad, and it is unclear how to satisfy the obfuscation requirement. It is also unclear whether the six categories are exhaustive or an illustrative list of possible obfuscating activities. If they are not exhaustive, then it is unclear what limiting principle applies to the rule, and what else might be covered. FinCEN should clarify the relationship between the "obfuscat[ing]" clause and the six categories.

Next, the six categories are overbroad in two ways. First, they encompass a wide range of activities that are not privacy-preserving—and therefore do not involve "mixing" as that term is naturally understood—at all. As written, they arguably encompass routine activities like standard Bitcoin UTXO transaction procedures, basic Ethereum smart contract functionality, and ordinary staking practices, none of which are primarily designed to enhance users' privacy. In other words, they appear to cover mainstream digital asset transactions. FinCEN should clarify that the proposed special measure does not apply to ordinary blockchain activities.

To the extent the categories do cover actual privacy-preserving technologies, they remain overly broad as most privacy-preserving technologies are not used primarily for money laundering or other illicit purposes. Nearly everyone wants a basic degree of privacy for their lawful activity. In the traditional-finance world, participants rely on privacy-preserving technology like password-protected accounts and encryption-protected communications because it is irresponsible to expose all affairs to the public.[31] Participants in the blockchain ecosystem need a similar degree of privacy for the same reason.

FinCEN must balance how much the covered transactions are "used for legitimate business purposes" with how much they are "used to facilitate or promote money laundering in or through a jurisdiction outside of the United States."[32] FinCEN cannot designate a class of activities as of primary money laundering concern if they are overwhelmingly lawful. As explained below, these six categories of activities, as written, are overwhelmingly lawful. They include most mainstream types of digital asset transactions. As FinCEN is aware, available data shows that digital asset transactions as a whole involve

[31] Of note, the importance of financial privacy is not a novel concept in the U.S. For instance, the Right to Financial Privacy Act of 1978 (RFPA) protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. *See* 12 U.S.C. §§ 3401-3423.
[32] 31 U.S.C. § 5318A(c)(2)(B).

less than 1-2 percent illicit transactions.[33] FinCEN should therefore not designate these broad categories as of primary money laundering concern.

1. *"Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction."*

As written, this category is overbroad. Many cryptocurrency activities involve using "code" to coordinate, manage, or manipulate the structure of a transaction. And as the term is generally understood, all or most of that code is "programmatic."[34] We believe that this category could arguably cover most software tools in the blockchain ecosystem.

A few examples illustrate the breadth of this category. First, in order to conduct an ordinary bitcoin transaction, a user typically uses programmatic code in the form of software that identifies and collects multiple unspent transaction outputs, or UTXOs, under control of the user's private key.[35] Such software is part of a standard bitcoin wallet offered as a convenience to users. The software exists for efficiency, not to facilitate improper activities. But because this software combines and splits digital assets to effectuate easy transactions, one could interpret that it falls within this category of "mixing."

Second, this category seems to encompass typical smart contracts, which are self-executing software deployed to a blockchain that make up decentralized protocols.[36] A smart contract might require multiple signatures to execute a transaction, or might include rules that coordinate transactions over time depending on certain inputs. Smart contracts like these are an integral part of the blockchain ecosystem. They are used by lawful businesses for lawful ends, like accomplishing a wide range of digital financial services in a disintermediated matter.[37] Such smart contracts have no particular connection to illicit finance. Yet they too appear to fall within this category.

Third, this category implicates one of the most promising frontiers of blockchain innovation, anonymity enhanced cryptocurrencies (AECs) and related privacy applications. AECs are designed to facilitate a safer and more attractive environment for digital asset transactions.[38] Instead of posting all aspects of every transaction on a public blockchain visible to anyone, many AECs use advanced math called "zero-knowledge proofs" to

---

[33] Norbert, *New Anti-Crypto Movement Escalates Congress's Assault on Privacy*, Forbes (Aug. 2, 2023), perma.cc/56RR-9VK7; *2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth*, Chainalysis (Jan. 18, 2024), perma.cc/W7R3-33V7 ("our estimate for the share of all crypto transaction volume associated with illicit activity also fell, to 0.34%"); *Financial Crime Typologies in Cryptoassets*, Elliptic (2020), perma.cc/67NZ-SNCW ("illicit activity today still accounts for less than 1% of all transactions"); *Crypto crime: Combatting hacks, thefts, and fraud in the decentralized finance ecosystem*, CipherTrace (June 13, 2022), perma.cc/64D2-JFME ("Illicit cryptocurrency activity is declining as a percentage of overall volumes" and accounts for 0.10-0.15% of total crypto volumes).

[34] *See Glossary of Coding Terms for Beginners*, Syracuse Univ., perma.cc/4D4C-H4MY (using "coding" and "programming" interchangeably).

[35] *See Understanding UTXOs - The Gold Coin Analogy*, Glassnode Academy, perma.cc/L6WJ-L8LT.

[36] *See Introduction to Smart Contracts*, Ethereum.org, perma.cc/D6VW-7AGB.

[37] *See What are smart contracts on blockchain?*, IBM, perma.cc/79YF-SWPN.

[38] *See* Wilcox, *Security and Privacy for Crypto with Zero-Knowledge Proofs*, a16z crypto (Aug. 29, 2019), perma.cc/6J3A-APZK; O'Sullivan, *What are mixers and "privacy coins"?*, Coin Center (July 7, 2020), perma.cc/J4G3-W9TQ.

securely validate transactions while leaving public information about those transactions in the users' control. They use code to allow users to control what aspects of their transactions are accessible, when, and by whom.[39] Therefore, they appear to fall within this category as well.

Furthermore, AECs and other privacy-preserving technologies are necessary to lawful users. The public nature of transactions on most blockchains makes users easy targets for theft, scams, retaliation, blackmail, kidnapping, and fraud. As discussed in more detail above, much like email encryption facilitated the mass adoption of email, emerging privacy-preserving technologies promise to facilitate the mass adoption of digital assets for lawful purposes. They bring into the blockchain ecosystem mainstream users and institutions who cannot otherwise use public-ledger technology. In other words, AECs represent a path to a more secure blockchain ecosystem. But this category treats them as of money laundering concern and threatens to cut off that path.

2. *"Facilitating user-initiated delays in transactional activity."*

As written, this category appears overbroad and counterproductive. First, this category also captures a wide range of lawful activity. User-initiated delays are a common and helpful way for users to plan their finances. Everyone is familiar with the importance of user-initiated delays from traditional finance, where people schedule payments or automate transactions in both their personal and business lives.[40] People use delay tools in traditional finance not because they are criminals but because doing so is sensible.

Cryptocurrency users initiate delays for similar reasons. They employ smart contracts that send payment when a later condition is met, escrow services that hold funds until a contract term is satisfied, and automated payments for subscriptions or donations.[41] These delay mechanisms serve important practical ends for responsible people to order their financial affairs, not for illicit finance. Unfortunately, this category seems to encompass them all.

Second, this category may be counterproductive. Some of the main tools used to prevent money laundering and illicit finance affirmatively require delay mechanisms. Delay mechanisms can help catch hackers and money launderers before their funds have been irreversibly transmitted. In other words, delays help prevent and reverse criminal activity. For example, mixing technologies can use withdrawal screening and de-anonymization procedures to delay the withdrawal of potentially illicit funds until or unless their legitimacy is confirmed.[42] FinCEN should avoid stifling such promising tools by classifying all such activities as of primary money laundering concern. Indeed, it would be directly

[39] *See* Ragsdale, *Privacy-Protecting Crypto Airdrops with Zero Knowledge Proofs*, a16z crypto (Mar. 27, 2022), perma.cc/D8LL-LUWN.
[40] *E.g.*, *Bill Pay: Schedule a Payment*, Chase, perma.cc/SD6W-8TPL.
[41] *E.g.*, *Create Escrow Smart Contract*, Medium, perma.cc/WE53-63WE; *Web3 Recurring Payments*, onchainpay, perma.cc/WVA4-K8PE.
[42] Burleson, Korver, & Boneh, *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs*, perma.cc/9K24-A4GV.

counterproductive to FinCEN's mission to fashion this special measure in a way that undermines or restricts use of such illicit finance mitigation functionalities.

3. *"Creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions."*

This category is not workable without further clarification. As written, it arguably describes the recommended good practice for all cryptocurrency users. A responsible cryptocurrency user commonly creates new addresses for new transactions.[43] Creating new addresses is simple, easy, and provides a bare minimum level of safety, security, and privacy. It also allows segregation of funds in support of sound compliance practices and basic accounting.[44] Nor does the requirement that a person engage in a "series of independent transactions" mitigate the problem. Good practices call for using separate wallets for separate—and therefore presumably "independent"—transactions. Further, new wallets are frequently seeded with funds via a regulated financial intermediary, where AML program requirements, including CDD and SAR reporting, already apply. Without further clarification about whether a series of transactions is "independent" or what that means, this proposal appears to capture entirely too much.

4. *"Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts."*

As written, this category encompasses activity fundamental to the lawful use of cryptocurrency. For example, users of many cryptocurrencies pool or aggregate tokens as part of the "staking" process. Stakers contribute digital assets to validators, which can be operated by centralized service providers or decentralized staking protocols. The process of staking acts as an economic pledge that the validator will function in accordance with the rules of the underlying blockchain network, with such validation activity being necessary for proof-of-stake blockchain networks to function.[45] Their ability to validate transactions and accomplish other essential tasks is a function of that stake. If users are not able to stake, then those blockchains will not function. Staking is routine and necessary. Yet, successful models *require* pooling digital assets from a wide range of persons in order to establish necessary decentralization. As a result, one could interpret the proposal's language to cover staking. Assuming that FinCEN does not intend this, it should very clearly clarify this; we assert that staking should specifically be excluded. Otherwise, labeling staking activities as a primary money laundering concern could result in a de-facto ban on blockchains.

This category also encompasses common practices like using liquidity pools. Liquidity pools are integral to decentralized finance and therefore to lawful crypto

---

[43] Frost, *Why you should always generate new Bitcoin addresses*, Decrypt (Jan. 24, 2020), perma.cc/WTM3-3HHU; *Why you should have multiple crypto wallets*, Moonpay (Dec. 7, 2023), perma.cc/ML9J-BHJZ.

[44] *How to manage multiple crypto wallets: Our best practices*, Request (June 6, 2023), perma.cc/ZEA2-CTRH.

[45] *Pooled staking*, Ethereum, perma.cc/6KLU-6LVY(last updated Oct. 25, 2023); Shimron, *Ethereum's Centralized And Decentralized Liquid Staking Providers Battle For Dominance*, Forbes (Jan. 21, 2023), perma.cc/KV8K-CXC3.

activities. They allow people looking to buy and sell assets to interact more efficiently. But, they operate by combining digital assets from multiple persons in one place to facilitate easy transactions, so they appear to fall within this category as written. Like staking, FinCEN should clarify that this routine activity is also not included.

Notably, these features enable decentralized exchanges, or DEXs, to operate autonomously pursuant to the conditions of the smart contracts and the decentralized participation of the system. DEX protocols allow users to exchange digital assets in a disintermediated and trustless manner, acting as one of the fundamental building blocks for the entire web3 ecosystem. The seamless exchange of tokens incorporated into all web3 applications – from social media to gaming and gig economy marketplaces – is as important to the emerging ecosystem as a common communications protocol was to the development of the Internet.

5. *"Exchanging between types of CVC or other digital assets."*

As written, this category appears to encompass mainstream and innocuous activity. Many cryptocurrency users exchange multiple types of digital assets. And a wide range of decentralized finance tools allow them to do so.[46] For example, someone who wants to trade ether for another cryptocurrency can do so through any number of decentralized protocols. Users take these steps for ordinary investment and utility purposes, like people in the traditional finance system who trade dollars for gold or stocks. Such trades are predominantly lawful and have no special connection to illicit activity. Yet they appear to fall squarely within this category. Moreover, a vast array of blockchain technologies that are outside of what is considered purely financial activity, such as services and transactions relating to NFTs and in-game assets for web3 video games could be covered.

Indeed, such decentralization accomplished through digital asset exchange enables innovations that are simply not possible to replicate through traditional, centralized systems. One of the true utilities of DEXs, for example, is that they act as a core primitive and infrastructure layer for all of web3, enabling the entire ecosystem of web3 applications, products, and services to utilize them in a manner that is seamless for the user. This will allow users to exchange their own assets into the assets of such systems through automatic routing without ever having to visit a centralized exchange or interact with an intermediary. Furthermore, DEXs enable trading of digital assets by bots, which help to provide stability to the entire web3 ecosystem. The United States will not be able to compete in the web3 economy of the future if DeFi systems aren't permitted to grow here.

FinCEN should narrow or clarify this category to reach only those patterns of exchange that closely correlate to illicit activity.

[46] Warren, *Decentralized Exchange*, Coin Center (Oct. 10, 2018), perma.cc/5MCP-ZM45; Ehrlich, *Crypto Exchanges: What Investors Need To Know*, Forbes (May 8, 2023), perma.cc/CPY4-LR6L.

6. *"Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions."*

Finally, FinCEN should clarify or narrow this category. It may be appropriate for FinCEN to impose reporting requirements akin to other laws governing users who structure transactions to avoid detection or separately-mandated reporting.[47] Many digital asset transactions, like transactions in traditional finance, are made through a series of independent transactions for other reasons. People make a series of independent transactions like the ones described by this category when they use a payment plan, for logistical convenience, because it is a standard good practice for privacy, or even because they are in an economic relationship that requires it—like a subscription or a lease. The fact of splitting and making separate payments should therefore not be enough to trigger a label "of primary money laundering concern" and additional reporting requirements. FinCEN should consider narrowing this category to more surgically target "structuring" as that category is understood in other areas of the law.

B. The exposure threshold exacerbates these problems.

The overbreadth problems are further exacerbated by the proposal's strong implication that it requires financial institutions to report transactions to which the financial institutions are not parties or intermediaries. By its terms, the proposal covers financial institutions' transactions that involve mixing, such as when someone runs their cryptocurrency through a mixer and then sends it directly from that mixer to a financial institution. But FinCEN's explanation of the proposal makes clear that it is seeking to regulate transactions involving digital assets that have *previously been* mixed or will *be mixed* in the future, even when the mixing and the financial institution are not part of the same transaction. The proposal calls this aspect of its reach "indirect exposure."[48] By requiring financial institutions to report indirect exposure, it turns them into investigators obligated to track transactions to which they are not a party into the past and future.

Specifically, the proposal says that it applies to all "CVC mixing exposure," which includes "direct exposure" *and* "indirect exposure." Direct exposure involves transactions where a covered entity receives or sends funds directly from or to a mixer—in other words, direct exposure happens when a financial institution is a party or intermediary to a mixing transaction.[49] But indirect exposure goes well beyond that. "Indirect exposure refers to transactions where CVC is sent from a CVC wallet address through at least one other wallet address to arrive at the intended recipient."[50] This includes when "CVC was sent from a CVC mixer to a CVC wallet address" in the past "and then to a VASP" as well as when "CVC sent from a VASP to a CVC wallet address was subsequently send [sic] to a CVC mixer" in the future.[51] The proposal offers no upper bound on the number of past and future transactions that it encompasses.

[47] E.g., 26 U.S.C. § 6050I(f); 18 U.S.C. § 1956(a)(1)(B)(ii).
[48] 88 Fed. Reg. at 72,717 & nn.121-22.
[49] *Id.* n.121.
[50] *Id.* n.122.
[51] *Id.*

The proposal then appears to confirm in several places that financial institutions must search for, collect, and report these transactions to which they are not themselves parties or intermediaries. It says that it "expect[s] covered financial institutions to employ a risk-based approach to compliance of this proposed rule, and more broadly, the Bank Secrecy Act, including by using the variously available free and paid blockchain analytic tools commonly available."[52] It applies when the financial institutions' "customers engage in a covered transaction," regardless of whether the financial institution is a party.[53] And because the premise of the proposal is that you cannot tell who controls funds that go through mixing services, it will require financial institutions to track the history and future of the digital asset itself, without knowing whether it belongs to a customer. It even says that financial institutions may be required to hire data analytic firms and do "supplementary manual investigative work to uncover" past and future transactions involving CVC mixing.[54]

Although the "indirect exposure" component of the proposal is mentioned only glancingly, it carries heavy implications. It expands the coverage of the proposal by increasing the number of covered transactions exponentially. It then increases the burden of compliance by requiring financial institutions to employ advanced investigation methods to trace each digital asset's history and future, which is complicated and costly. And it introduces indecipherable uncertainty by not saying how far into the past and future financial institutions, now deputized as investigators of their customers' separate transactions, must go.

This indirect-exposure component expands the underlying statutory authority beyond its intended scope. As described in more detail below, Special Measure 1 allows FinCEN to mandate reporting information about transactions in which a financial institution is a party or intermediary.[55] But there are serious questions about whether it allows FinCEN to mandate investigating and collecting information about transactions to which it is neither a party nor intermediary, and in which its customers may well not even be involved. Special Measures 2 through 5 govern FinCEN's authority to require financial institutions to affirmatively "obtain" new information in an investigative capacity, but those Special Measures include further elements not satisfied here.[56] By repurposing Special Measure 1 to accomplish a collection of records not authorized under the measures that specifically authorize information collection, the proposal exceeds Congress's design.

C. The foreign-nexus requirement exacerbates these problems.

The proposal applies to transactions "within or involving a jurisdiction outside the United States."[57] Although this foreign-nexus requirement at first may appear meaningful, we are concerned that it will not turn out to be so in practice.

---

[52] *Id.* at 72,710.
[53] *Id.* at 72,708.
[54] *Id.* at 72,717.
[55] 31 U.S.C. § 5318A(b)(1).
[56] 31 U.S.C. § 5318A(b)(2)-(5).
[57] 88 Fed. Reg. at 72,722.

Most blockchain activities arguably implicate participants all over the world. Ordinary transactions by Americans can technically include foreign servers, foreign validators, foreign participants in decentralized exchange, or foreign participants in a decentralized autonomous organization.[58] The decentralized, accessible nature of blockchains means that many transactions arguably implicate foreign jurisdictions, even when those transactions are for all practical intents and purposes controlled by Americans.

Furthermore, the nature of the public ledger makes it difficult or impossible to determine the location of others involved in CVC activities. Often a transaction will involve, or be validated by, actors identified only by a pseudonymous address.[59] Sometimes that address cannot be traced to an identifiable individual. Even when it can, identifying that individual does not reveal the location. The proposal acknowledges this reality in other contexts.[60] Therefore, any transaction *might* involve someone in a foreign jurisdiction, so domestic transactions will usually be impossible to distinguish from foreign transactions.

The proposal does not explain how to account for these problems. Instead, it confirms the problem: it says financial institutions must presume that every CVC transaction is covered, even when nothing suggests foreign involvement. In the words of the proposal, "the implied burden would shift from determining when a CVC transaction is reportable to determining when it is not reportable."[61] As a result, every *American* who uses a "mixing technology," as defined by the six broad categories, will likely be covered. In effect, this regulation targets primarily domestic transactions rather than the genuinely foreign transactions for which the statute was designed.

D. The special measure will operate as a de facto ban on many blockchain and CVC activities.

We believe that the proposal may effectively ban financial institutions from dealing with most digital assets.

When FinCEN designates a class of activities as of primary money laundering concern and requires associated recordkeeping and reporting, it largely severs financial institutions' ties with people and businesses who engage in those transactions. The proposal's "primary money laundering concern" designation tells financial institutions to treat industry players, including ordinary digital asset businesses, as operating a risky and legally perilous line of business. Through their risk-based assessment practices, they will therefore often decide that they should not offer banking and similar services to these businesses. In FinCEN's own words, "it is reasonable to expect that the relative attractiveness of engaging with CVC mixers or the number of those who avail themselves of

[58] *E.,g., Global Bitcoin Nodes by Country*, Bitnodes, perma.cc/NPV7-QYXV.
[59] Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 6 (2009), perma.cc/Y7KD-JJNX.
[60] 88 Fed. Reg. at 72,709 ("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.").
[61] *Id.* at 72,713.

CVC mixing services might be affected."[62] In more concrete terms, lawful blockchain businesses and activities will be choked out of the economy.[63]

Making matters worse, the proposal will require considerable investigative efforts on a huge scale to track customers' past and future crypto use. And it will be legally risky because of the uncertainty surrounding the proposal's scope and meaning. Given these costs and risks, we expect financial institutions to further isolate or even sever ties with cryptocurrency-related businesses and users. They could refuse to process transactions involving digital assets, to custody digital assets, and even to provide ordinary bank accounts for cryptocurrency-associated companies, thereby making it impossible for them to survive in America.

The proposal does not appear to fully grapple with these implications. Rather than treat the proposal as a marginal cost increase to covered financial institutions, FinCEN should treat the proposal as a potentially existential threat to much of the blockchain and web3 economy and to thousands of American jobs. Doing so would likely change FinCEN's balancing of the statutory factors, impact analysis, and cost assessments.[64]

IV. The proposed special measure raises significant litigation risks.

In light of these concerns, we believe that the proposal is vulnerable to challenges in court. We are hopeful that FinCEN will revisit the proposed special measure before publication, but will briefly explain our primary legal concerns with the proposal as it stands today.

We believe that the proposal cannot be reconciled with the statutory factors. Under Section 311 of the Patriot Act, FinCEN must balance how much the classified transactions are "used for legitimate business purposes" with how much they are "used to facilitate or promote money laundering in or through the [foreign] jurisdiction."[65] This statutory balancing requires FinCEN to recognize and account for the legitimate activities that its class of transactions encompasses. It also prevents FinCEN from designating a class of activities as of primary money laundering concern if those activities are overwhelmingly legitimate.

Here, FinCEN's assessment of the statutory factors appears inadequate because it did not recognize the breadth of legitimate activities that its categories encompass. For example, FinCEN stated that "the number of transactions that would require reporting and recordkeeping as a unique consequence of adopting special measure one as proposed is extremely low in relative terms." But based on the text of the proposal, that number is in fact extraordinarily high—in both absolute and relative terms. Likewise, a more fulsome analysis would have concluded that the six categories of covered activities, as currently described, are overwhelmingly legitimate—and therefore not a proper class for

[62] *Id*. at 72,716.
[63] *Cf. Operation Choke Point 2.0: The Federal Bank Regulators Come For Crypto*, Cooper & Kirk, perma.cc/UKT4-GQEY.
[64] *See* 88 Fed. Reg. at 72,704-07; 72,708; 72,713-19.
[65] 31 U.S.C. § 5318A(c)(2)(B).

designation—because they involve largely mainstream and licit digital asset activities. FinCEN's statutory balancing is likely contrary to law and an abuse of discretion.[66]

We also believe that FinCEN may lack clear statutory authority to take this action for multiple reasons:

- The proposal effectively overrides Section 311's foreign-nexus requirement, which imposes a crucial limitation on FinCEN's otherwise broad statutory authority. The proposal applies to a class of transactions for which any foreign nexus cannot be discerned, so it effectively regulates all American transactions. FinCEN advises financial institutions to flip the burden and assume that the foreign nexus requirement is satisfied.[67] But the statutory text demands a foreign nexus and does not authorize this effectively unlimited domestic application.[68]

- The proposal requires financial institutions to create and report records of transactions to which they are not parties or intermediaries. It requires financial institutions that deal with digital assets to investigate whether the assets that they handle have been used in mixing transactions at other times, and then to monitor how those assets are used into the future. It is therefore akin to a rule that requires banks to put cameras or GPS devices on the dollars that they handle and then report to FinCEN what their customers (or others) do next. We are aware of no authority for FinCEN to extend its jurisdiction, through deputized financial institutions, to transactions happening fully beyond their reach.[69]

- The proposal transforms Special Measure 1 into a tool for investigating and banning transactions, not a mere recordkeeping and reporting requirement. By its terms, Special Measure 1 authorizes FinCEN to require financial institutions only to "maintain records" and "file reports" about transactions.[70] It stands in contrast to Special Measures 2 through 5, which authorize FinCEN to require financial institutions to take further steps, including to affirmatively "obtain … information" not already in their possession or to outright "prohibit" certain actions.[71] Because they authorize these more aggressive steps, Special Measures 2 through 5 impose other, more demanding conditions on their exercise.[72] But as explained above, the proposal does not merely require financial institutions to maintain and

[66] *See* 5 U.S.C. § 706(2)(A), (C); *Citizens Coal Council v. EPA*, 385 F.3d 969, 977 (6th Cir. 2004) ("an agency abuses its discretion when it fails to consider a factor the statute directs it to consider in promulgating regulations"); *Simms v. NHTSA*, 45 F.3d 999, 1008 (6th Cir. 1995) ("An agency may only act within the scope of its authority as conferred by statute.").
[67] 88 Fed. Reg. at 72,713.
[68] *See* 31 U.S.C. § 5318A(b).
[69] *See* 31 U.S.C. § 5318A.
[70] 31 U.S.C. § 5318A(b)(1).
[71] *Id.* § 5318A(b)(2)-(5).
[72] *See id.*

> report records that they already have, like a bank account with its own books; instead it requires them to use investigative methods to affirmatively "*obtain*" new information, write narratives, and create new records to report. It also, in practice, bans financial institutions from dealing with the covered transactions. Because courts "assume that Congress 'acts intentionally and purposely' when it 'includes particular language in one section of a statute but omits it in another section of the same Act,'" we do not believe that Special Measure 1 should be read to authorize the affirmative investigation and effective prohibition that Congress intended to govern through Special Measures 2-5.[73] But the proposal turns Special Measure 1 into a supercharged power that swallows the others.

In this context, FinCEN's statutory authority must be clear. The proposal, as written, arguably triggers the major-questions doctrine because it involves an economic and political question that could determine the direction of the $1 trillion digital asset industry and that requires the reporting of potentially millions of transactions.[74] And, the proposal will be subject to the rule of lenity because it sets obligations enforceable with criminal penalties.[75]

Next, the proposal may be vulnerable to an arbitrary-and-capricious challenge.[76] It relies on inconsistent data analysis and other errors that may warrant vacatur. For example, FinCEN justified the proposal because it says that in 2022, 24% of the total transaction volume processed by mixers came from illicit sources, whereas only 10% did in 2021.[77] But elsewhere, FinCEN suggests that "because of the lack of available transactional information, FinCEN cannot fully assess the extent to which, or quantity thereof, CVC mixing activity is attributed to legitimate business purposes."[78] Worse, the 24% estimate represents the proportion of transactions involving "CVC mixers." But the proposal covers "CVC mixing," which FinCEN itself acknowledges is a separate and larger category.[79] More fundamentally, this estimate appears to assume that CVC mixing will *not* include the many standard blockchain activities discussed above, but that assumption cannot be reconciled with the proposed text. If FinCEN properly calculated the number of transactions affected, as

---

[73] *Polselli v. IRS*, 143 S. Ct. 1231, 1237 (2023).

[74] *See Util. Air Regulatory Group v. EPA*, 134 S. Ct. 2427, 2444 (2014) ("We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast "economic and political significance.""); Chavez-Dreyfus, *Crypto market cap surges to record $2 trillion, bitcoin at $1.1 trillion*, Reuters (Apr. 5, 2021), perma.cc/97NN-62KB; *but see Securities and Exchange Commission v. Terraform Labs Pte. Ltd.*, 2023 WL 4858229, (S.D.N.Y. July 31, 2023). Judge Rakoff recently concluded that the blockchain industry lacks vast economic and political significance, reasoning that "it would ignore reality to place the cyrpto-currency industry and the American energy and tobacco industries . . . on the same plane of importance." *Id.* at *8. The court's analysis, however, is not only empirically unfounded, but impossible to square with the Supreme Court's recent decision in *Biden v. Nebraska*, which looked at the financial magnitude of a regulatory action, not its resemblance to the character of the industry in question. 600 U.S. 477 (2023).

[75] *See* 31 U.S.C. § 5322; *Cargill v. Garland*, 57 F.4th 447 (5th Cir. 2023) (en banc), *cert. granted*, 2023 WL 7266996 (Nov. 3, 2023); *Romero v. DHS*, 20 F.4th 1374 (11th Cir. 2021).

[76] *See* 5 U.S.C. §706(2)(A).

[77] 88 Fed. Reg. at 72,706.

[78] *Id.* at 72,707.

[79] *Id.* at 72,706 n.69.

required by statute, we believe that a far smaller percentage of covered transactions would involve illicit sources.[80] As detailed in sections III. B. and C. above, the proposal's indirect exposure and foreign nexus requirement provisions alone make cost estimates significantly lower than reality. FinCEN's failure to undertake a comprehensive and accurate impact analysis will be scrutinized by courts. An agency decision based on an incomplete economic analysis of the impacted "industry" or on "conflicting record data" is "not the product of reasoned decisionmaking" and therefore arbitrary and capricious.[81]

The proposed special measure also appears to not consider a wide range of important factors, including its implications for several types of activities that its terms cover, but it does not address, how the impossibility of discerning a foreign nexus will affect the number and nature of reportable transactions, and the extent to which it will effectively ban promising new technologies. We believe that the APA requires a stronger justification and more comprehensive analysis.[82]

Finally, the proposal could implicate constitutional issues. It requires large-scale reporting of sensitive information and expressive associations, which may make it subject to facial or as-applied challenges under the First and Fourth Amendments, both of which set hard limits on the government's ability to forcibly collect that information.[83]

V. We recommend a more surgical regulatory strategy.

We believe that a narrower approach would mitigate the harms that we have identified and better serve FinCEN's goals.

First, in terms of targeted activities, we recommend identifying mixing entities or technologies specifically and by name, rather than through broad generic descriptions that inevitably capture other activities and raise vexing interpretive and compliance questions. We also recommend targeting only those activities and services used primarily for illicit purposes, or only in conjunction with other, independent indicia of illicit activity. For example, instead of targeting all transactions that involve "pooling" digital assets, FinCEN might have done something like the Office of Foreign Assets Control did when it targeted transactions that went through the "Blender.io" mixing service.[84] Better, FinCEN might have targeted only those Blender.io (or similar) transactions likely to be illicit, such as those that involve large sums of digital assets and complex obfuscatory methods.

Second, we recommend that FinCEN limit its coverage to transactions to which a financial institution is a party or an intermediary, rather than requiring financial

---

[80] *E.g.*, Norbert, *New Anti-Crypto Movement Escalates Congress's Assault on Privacy*, Forbes (Aug. 2, 2023), perma.cc/56RR-9VK7 (estimating 1% of crypto use illicit).
[81] *Tel*Link v. Fed. Commc'ns Comm'n*, 866 F.3d 397, 415 (D.C. Cir. 2017).
[82] *See,* 5 U.S.C. §706(2)(A); *see, e.g.*, *Transp. Div. of the Int'l Ass'n of Sheet Metal, Air, Rail & Transp. Workers & Bhd. of Locomotive Eng'rs & Trainmen v. Fed. R.R. Admin*., 40 F.4th 646, 656 (D.C. Cir. 2022) (""A rule is arbitrary and capricious if an agency fails to consider a factor [it] must consider under its organic statute."); *Nat'l Parks Conservation Ass'n v. EPA*, 788 F.3d 1134, 1141 (9th Cir. 2015) ("an internally inconsistent analysis is arbitrary and capricious").
[83] *See Bonta*, 141 S. Ct. 2373; *Carpenter*, 138 S. Ct. 2206.
[84] 88 Fed. Reg. at 72,703 n.25.

institutions to investigate and police separate transactions into the past and future. We urgently recommend that, if FinCEN goes beyond such transactions, it clarifies how far financial institutions must go into the past and future, either in terms of time or the number of transactions.

Third, as to the foreign-nexus requirement, we recommend that FinCEN clarify that a transaction involves a foreign nexus only when it involves *parties*—not validators or other actors incidentally connected to the transactions—who can be readily identified as foreign. We recommend a presumption that for most American financial institutions, their customers are usually American and should not be treated as satisfying the foreign-nexus requirement absent further evidence.

Fourth, we recommend that FinCEN exempt from designation as a "mixing service" and of primary money laundering concern those privacy-preserving technologies that introduce and maintain protective measures such as time delays, deposit limits, sanctions screening, KYC procedures, SAR filing, and other techniques and practices which could prevent illicit activities by blocking or deterring use of the technologies by bad actors.[85]

Fifth, as a means of accomplishing FinCEN's goals, we believe that Suspicious Activity reporting and similar actions will do so with greater clarity, precision, and effectiveness than broad regulations like the proposed special measure. For example, reformatting the SARs to include specific categories and box checking for blockchain-related data and types of associated suspicious activity such as presence of money laundering techniques and activities that may be prevalent with digital assets. Also, enabling and encouraging the filing of SARs by a wider group of individuals and entities than those that are legally BSA obliged would increase useful and relevant intelligence and evidence to FinCEN and law enforcement.

Finally, a new or clarified special measure proposal should give regulated parties an opportunity to respond through a new comment period. "While a final rule need not be an exact replica of the rule proposed in the Notice, the final rule must be a 'logical outgrowth' of the rule proposed."[86] "Clearly, 'if the final rule deviates too sharply from the proposal, affected parties will be deprived of notice and an opportunity to respond to the proposal.'"[87] This requirement is especially strong in the Section 311 context, where FinCEN must "provid[e] and enabl[e] [regulated parties] to respond to all the public information upon which FinCEN relied."[88] And it must "explain[] in the rule why potentially viable but less drastic alternative penalties were not chosen."[89] Further, FinCEN should provide a

[85] Importantly, zero-knowledge proofs, the technical methodology that underlies many privacy-preserving products and services, can be designed and used to mitigate illicit finance and national security risks. Current research suggests that there are a number of possible methods for privacy-enhancing products and services to mitigate risk. *See e.g.* Burleson et al., *supra*, perma.cc/9K24-A4GV.

[86] *National Black Media Coalition v. F.C.C.,* 791 F.2d 1016, 1022 (2d Cir. 1986) (quoting *AFL-CIO v. Donovan*, 757 F.2d 330, 338 (D.C. Cir. 1985); *United Steelworkers v. Marshall*, 647 F.2d 1189, 1221 (D.C. Cir. 1980), *cert. denied sub nom., Lead Industries Ass'n v. Donovan*, 453 U.S. 913, 101 S.Ct. 3148, 69 L.Ed.2d 997 (1981)).

[87] *National Black Media Coalition v. F.C.C.,* 791 F.2d 1016, 1022 (2d Cir. 1986).

[88] *FBME Bank Ltd. v. Lew*, 125 F. Supp. 3d 109, 114 (D.D.C. 2015).

[89] *Id.*

reasonable sunrise period for covered entities to establish methods for any additional or novel reporting that may be required.

The proposal, as written, covers such a vast number of possible transactions that its implications cannot feasibly be explained and its economic implications cannot accurately be calculated. Given the lack of information about most of the covered activities, as well the numerous potentially viable but less drastic approaches that we have outlined, a new comment period for a modified special measure proposal is especially important here.

VI. Conclusion

A16z appreciates the opportunity to share its perspective on this proposed special measure. We hope that you find our suggestions useful for the rulemaking process, and we look forward to continued engagement with FinCEN on these issues.

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z

Miles Jennings, General Counsel and Head of Decentralization
a16z crypto

Michele R. Korver, Head of Regulatory
a16z crypto

Brian Quintenz, Global Head of Policy
a16z crypto