VIA REGULATIONS.GOV

January 22, 2024

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

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

Dear Director Gacki,

The Crypto Council for Innovation ("CCI") submits this letter in response to a request for comment regarding the United States Department of the Treasury Financial Crimes Enforcement Network's ("FinCEN") Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern ("proposed rule" or "proposal" or "NPRM"). CCI appreciates the opportunity to (i) share its information, expertise, and views on this vital issue and (ii) to be a resource to FinCEN. Digital assets represent one of the most significant innovations in finance—and beyond—with the existing ability and continued potential to enhance ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security. The responsible development of the digital assets ecosystem, therefore, is an important priority for policymakers.

I. Summary

This proposal differs from FinCEN's predominant use of its authority under Section 311 of the USA PATRIOT Act, in which it typically targets a specific entity or jurisdiction. Importantly, using Section 311 to designate a class of transactions requires precision and clarity to ensure that covered entities can implement the requirements and meet the objective of deterring illicit finance. We urge FinCEN to proceed with caution when applying this authority to an entire class of transactions. To that end, CCI would like to raise eight key areas of concern with the NPRM that not only make the requirements potentially infeasible for covered financial institutions but also could undermine FinCEN's goal of mitigating illicit finance. These areas of concern center around the current language of the proposed rule that:

A. define mixing service and mixer too broadly and would force covered entities to over-extend the reporting requirements to capture commonplace, non-illicit activities;

B. make it infeasible to confine reporting only to activities involving jurisdictions outside the United States, and therefore would cause institutions to make reports that exceed statutory authority;

C. create duplicative and overly-burdensome work for covered institutions that would already be reporting much of the same activity under current suspicious activity reporting rules;

D. create conflicting standards with respect to the data-gathering processes of blockchain analytics firms, and in turn, conflicting reports about what activity should be considered "suspicious" or reportable under the NPRM;

E. cause unnecessary incursions into customer privacy and make customers, financial institutions, and FinCEN more vulnerable to a variety of financial and cyber-based threats from malicious actors;

F. lack data and analysis on the levels of lawful transaction activity associated with privacy-enhancing technologies;

G. stifle private sector innovation; and

H. create a regulatory mismatch between the U.S.and other jurisdictions, pushing crypto activity offshore and undermining U.S.law enforcement access to financial crime leads.

In light of these concerns, CCI respectfully recommends the below amendments to the current FinCEN proposal:

A. FinCEN should prevent the massive reporting of unhelpful information by narrowing reporting requirements to transactions with "a CVC service that indiscriminately facilitates illicit transactions by obfuscating their origin, destination or counterparties." FinCEN should also provide further guidance on exceptions from reporting as to not capture legitimate privacy enhancing activities of financial institutions (FIs).

B. FinCEN should give clear guidance for how FIs should ascertain when transactions involve mixing "within or involving a jurisdiction out of the United States." Such guidance should include, for example, technical methods and procedures covered institutions should employ to stay within the statutory boundaries of the Special Measures.

C. FinCEN should add a field for mixer data in the Suspicious Activity Report (SAR) form and eliminate the need for the "Narrative" field in the proposed regulations since such a field would already exist when a SAR is filed. If FinCEN wants to eliminate the SAR filing threshold, it should propose a rule directly on that point and provide a collateral impact analysis for dedicated notice and comment.

D. FinCEN must help establish industry standards for blockchain analytics in order to ensure accurate and consistent data since covered institutions would rely on such data to comply with the NPRM. Institutions should not be penalized for misaligned data gathered from different blockchain analytics firms.

E. In order to most efficiently and effectively target money laundering and limit the compliance burden for FIs, FinCEN should consider establishing a $10,000 volume threshold for reporting mixing services transactions, similar to currency transaction reports. FinCEN should narrow reporting requirements to direct exposure to mixers and exclude indirect exposure. Also, FinCEN should ensure that the channel it establishes for NPRM-required data from financial institutions operates under the same level of security and protection as provided by the Bank Secrecy Act (BSA) E-Filing System.

F. FinCEN should conduct a study on lawful and/or low-risk transactions with the types of tools potentially covered by the NPRM and publish the findings.

G. FinCEN should host a tech sprint on privacy-preserving compliance solutions to encourage private sector innovation on compliant privacy-enhancing technologies. Also, FinCEN should allow for private sector experimentation through exceptive relief and regulatory sandboxes.

H. FinCEN should seek to align the proposed rules with the recommendations offered by international standard-setting bodies such as FATF and pursue risk-based approaches to privacy-enhancing technologies. FinCEN must take a global approach to ensure U.S. law enforcement is not at a disadvantage when investigating financial crime for an ultimately borderless technology.

II. Detailed Discussion

A. *The NPRM's proposed definitions of "CVC mixing service" and "CVC mixer" are overly broad, and will unnecessarily capture commonplace and lawful activities and stray from FinCEN's stated goals of targeting illicit activity.*

i. The sweeping definitions of both "CVC mixing service" and "CVC mixer" **capture a wide variety of services that are not suspicious obfuscation. The 'Exception' is not broad enough to capture legitimate and lawful use cases.** Defining CVC mixing as "the facilitation of CVC transactions in a manner that **obfuscates** the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used," can apply to a wide variety of services that have no primary purpose or intention to obfuscate (like a tunnel through a mountain obscures a car license plate from above, but is not the purpose of the tunnel). As FinCEN acknowledges in the NPRM, defining a CVC mixer as "any person, group, service, code, tool, or function that facilitates CVC mixing" is broad.[1]

a. The proposed definition makes no distinction around where the obfuscation actually occurs; it also makes no distinction around whether it is ancillary or a primary function of the mechanism, and from whom. Technically, a compliant centralized exchange's activities could fall under this definition for its off-chain wallet management that is obscured from the public blockchain or for offering pooling or staking services. Similarly, any financial institution that batches transactions could potentially fall within the proposed definition.

b. The NPRM's limited exemption for the internal processes used by FIs to execute transactions as a general business operation demonstrates the ambiguity of this definition as well as the fact that exemptions will be continuously needed to accommodate technological developments. While covered institutions may find that they may not need to report on transactions with well-known virtual asset service providers (VASPs) that are exempted from the application of the rule, the NPRM does not offer clear and objective standards to determine a VASP's exemption status.

ii. **The breadth of the proposed definitions runs the risk of capturing commonplace transactions with digital assets.**

[1] FinCEN, "Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern" 88 FR 72701, 72709 at (Oct. 23, 2023) (Proposed Rule).

a. For example, "exchanging between types of CVC or other digital assets" or "facilitating user-initiated delays in transactional activity" could implicate over-the-counter (OTC) traders who are using those techniques to conduct more efficient trades. Again, it is not clear how regulated, compliant OTC business activity would be exempted from being reported as mixing transactions, even though mixing is neither their primary purpose nor a meaningful risk. The rule should not presume illicit activity by regulated entities; compliance effectiveness is a matter for international standards implementation, not presumptive suspiciousness reporting that could lead to unpredictably broad de-risking.

    1. In addition, certain blockchain transactions use time delays to prevent illicit finance (e.g., through smart contracts that check that funds do not come from criminal activity). A user executing such a contract could be considered making a user-initiated delay even though the action's intention would be to mitigate illicit transactions.

iii. Furthermore, "[c]reating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions" may be done by financial institutions for legitimate privacy and security operations (and even accounting segregation) purposes. Many self-custody wallets operate through single use addresses by default. Often, covered institutions see their customers consolidating the funds from all such wallets into one single custodial wallet on the institution's platform and would not generally view this practice as mixing. While such activities might superficially obscure some of the history of funds, they do not hide that history from basic analysis tools. The proposed definitions do not make any distinction around what level of obfuscation should fall under mixing, making it applicable to the most mundane of transaction activities. The 'Exception' should, at the very least, also include the use of internal protocols or processes to execute transactions *and* perform lawful privacy enhancing and security operations for customers.

iv. As stated in the NPRM, FinCEN needs to take into consideration the undue cost and burden associated with additional compliance for financial institutions without a commensurate law enforcement objective. The volume of transactions that would be considered having exposure to 'CVC mixing' and 'mixing services' under the proposed broad definition could impose a significant operational compliance burden on FIs. Requiring institutions to report on any transaction with exposure to mixing as broadly defined under the proposed rule, with no threshold amount or limitation to direct exposure, could potentially be interpreted as requiring centralized exchanges and platforms to report on nearly every digital asset transaction that occurs on their platform. The compliance burden is difficult to quantify, but would undoubtedly be extremely costly, and unworkable with the lack of clarity around what transactions this proposed rule would truly encompass. For a platform or exchange that engages in a high volume of transactions, this new reporting process would require an entire team to manage, estimated around 50 new headcount. The activity FinCEN is attempting to capture must be explicitly narrowed for many reasons, but especially from an operational compliance perspective.

v. This proposed rule seems to assume that all transactions related to mixing are illicit or suspicious, and hence, all transactions with exposure to mixing services should be reported to FinCEN. This frequently is not the case. More specifically, there are many examples of legitimate and lawful privacy enhancing activities that might constitute as suspicious and reportable "CVC mixing" due to the proposed rule's overly broad definitions.

    a. There are lawful use cases for mixers for U.S. consumers today. For example, several large U.S.companies offer to pay their employees in digital assets, including some CCI members. Many other companies offer consumers the option to convert their paychecks into cryptocurrency. Highly visible figures including professional athletes and elected politicians have acknowledged publicly that they would convert some of their salaries into crypto. Cryptocurrency wallets holding such funds offer insights into the user's salary, wealth and spending history. Mixing technologies–even those of minimal complexity such as generating single use addresses–act as a privacy tool to limit the exposure of one's holdings in cryptocurrency wallets from being broadcast in aggregate on the blockchain, otherwise making wallet-holders a target for hackers, identity theft, and financial fraud. Without mixing services, it would not be possible for consumers who are paid in cryptocurrency to maintain financial privacy.

b. FinCEN also recognizes in the NPRM that "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."[2] Those legitimate purposes, however, are not excluded from reporting under the proposed rule. The proposal needs to make a distinction between legitimate and illicit mixing activity.

vi. **The current scope of CVC mixing definitions risks implicating the blockchain base layer, jeopardizing the neutrality of the foundational infrastructure and compromising its integrity and core functionality.** Designating a set of crypto transactions could unnecessarily implicate blockchain technology infrastructure providers including builders, pool operators, relays, searchers, sequencers, and validators who could be deemed to provide "mixing services."

a. The proposed rule does not define parameters around what determines "obfuscating the source, destination, or amount" of a CVC transaction. With this lack of clarity, there is the possibility that these key infrastructure activities, which operate in an automated, permissionless manner – in some instances, the equivalent of ISPs or communications data packet-switching – could be viewed as mixing. Such an interpretation would require every blockchain transaction facilitated by a covered institution to be reported to FinCEN.

CCI proposes the language in the regulatory text regarding *CVC mixing* include the bolded language below:

> "(3) *CVC mixing.* (i) The term "CVC mixing" means the facilitation of CVC transactions **on the blockchain that indiscriminately facilitates illicit transactions by obfuscating** ~~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…"

We propose the language in the regulatory text regarding *Exceptions* be amended to include the bolded language below:

> "(ii) *Exception.* Notwithstanding paragraph (a)(3)(i) of this section, CVC mixing does not include the use of internal protocols or processes to execute transactions **or provide licit privacy-enhancing features** by banks, broker-dealers, or money services businesses, including virtual asset service providers that would otherwise constitute CVC mixing…"

CCI Recommendation: FinCEN should sharpen the applicability of this authority by defining reportable mixing as transactions with "a CVC service that indiscriminately facilitates illicit

[2] Proposed Rule at 72706.

transactions by obfuscating their origin destination or counterparties." This uses the exact language that Treasury used to describe the activities of the first mixing service it ever designated (Blender.io), in 2022.[3] This definition would also focus on transactions that are considered illicit on a reasonable basis and prevent massive reporting of unhelpful and unneeded information for AML/CFT purposes. FinCEN should also provide further guidance on what would be exempted from these definitions, which would enable lawful privacy-enhancing technologies and business' operational functions to continue to function.

B. Confining reporting to transactions with a nexus to jurisdictions outside the United States is logistically difficult and requires more guidance for institutions to not exceed statutory authority.

i. FinCEN Special Measures authority only extends to classes of transactions "within, or involving, a jurisdiction outside of the United States." Therefore, any financial institution that reports to FinCEN any class of transactions without clear knowledge that they are within, or involving, a jurisdiction outside of the United States could run the risk of exceeding the Special Measures mandate and create potential regulatory, civil liability, and litigation concerns. Thus, financial institutions may not always be in a position to report the mixing activity in question. Note that the reporting envisioned by the NPRM does not extend financial institutions the type of suspicion-based safe harbor that is afforded under the SAR regimes.

CCI Recommendation: FinCEN should clarify how it intends financial institutions to know or ascertain when transactions involve mixing "within or involving a jurisdiction out of the United States." In particular, guidance should include technical methods and procedures covered institutions should employ to stay within the statutory boundaries.

C. The NPRM's proposed reporting requirements are overly burdensome and will constitute a significant and in many cases duplicative burden for FIs, particularly since existing regulations already mandate reporting on suspicious activity.

i. Given the fact that the BSA already subjects covered institutions to substantial reporting requirements around suspicious activities, new reporting requirements under the proposed regulations would be duplicative.

a. In many cases, covered financial institutions will still have to file SARs in addition to submitting separate NPRM-mandated reports on transactions linked to identified or suspected mixers.

[3] *See* https://home.treasury.gov/news/press-releases/jy0768

b. For example, under the current SAR regime, the use of an intermediary wallet in what appears to be an attempt to circumvent reporting is already considered a suspicious, reportable event.

    1. Under the NPRM, SARs will capture exactly the same information, including a narrative. Therefore, the NPRM appears to propose a duplicative, parallel SAR regime with potentially much shorter timelines since the detection of a transaction with a known mixer is likely to be immediate whereas with SARs, institutions may take a few weeks to determine if activity is suspicious. The proposed rule would effectively seek to change how suspicious activity is reported without following the process to update the SAR regulations.

    2. Additionally, prior to the imposition of the Special Measures, many covered institutions may have already taken a view that certain activity involving mixers was considered a suspicious, reportable event.

c. FinCEN's categorization of foreign mixing activity as being of primary money laundering concern will also likely lead to more SARs being filed on such activity. Thus, the proposed reporting requirement will not only increase the number of mixing-specific reports filed pursuant to the new rules, but also the number of SARs filed on mixing. These reports will be duplicative and thus not helpful to law enforcement.

ii. The narrative field in the proposed reporting form would significantly increase hours and labor for compliance teams because drafting responses in those fields could not be fully automated. Having an open-ended narrative will also create inconsistencies in covered institutions' reports and make it harder for FinCEN examiners to easily identify suspicious activity. We would recommend removing this field.

iii. The NPRM's proposed reporting requirements also must reconcile with the Paper Reduction Act ("PRA"). The PRA implementing regulations at 5 CFR 1320.5(d)(1)(ii) and 5 CFR 1320.9(b) direct federal agencies to specify whether the proposed collection of information "is not unnecessarily duplicative of information otherwise reasonably accessible to the agency." The NPRM does not appear to comply with the PRA as SARs would capture and make accessible to FinCEN most, if not all, of the information that would be collected by the NPRM's proposed reporting requirements.

iv. The proposed regulations' imposition of overly broad and burdensome reporting requirements on exchanges would increase the time, effort, and technical tools needed to conduct blockchain analysis.

a. Given the broad definitions of "mixing services" and "CVC mixers," and the wide range of activities that they span, covered institutions would likely have to engage in expansive on-chain monitoring in order to identify shifts in wallet activity that could fall within the scope of the proposed definition. For example, even wallets associated with a low-risk institutional client with transparent and well-known business activity may prompt scrutiny when interacting with new wallets or implementing new wallet security procedures.

b. The increased technical sophistication of blockchain analysis tools needed to (a) capture the breadth of activity and (b) attribute "mixer" status to otherwise common data processing or protection processes, coupled with the need for constant evaluation would make compliance with the new requirements prohibitively expensive for covered institutions.

CCI Recommendation: FinCEN should add a field for mixer data in the Suspicious Activity Report form. This would also eliminate the need for the "Narrative" field in the proposed regulations since such a field would already exist when a SAR is filed. Duplicative reporting that does not add value should be avoided. If FinCEN wants to eliminate the SAR filing threshold, it should propose a rule directly on that point and provide a collateral impact analysis for dedicated notice and comment.

D. Given different standards and methods used by blockchain analytics providers, covered entities' reliance on these firms to comply with the NPRM's proposed rules will result in conflicting reports and potentially increase the risk of noncompliance if FinCEN relies on different blockchain analytics firms.

i. By enforcing increased or necessary reliance on these private companies without first establishing industry standards and requirements, the government may unintentionally encourage inconsistent and inaccurate reporting. At the peril of being out of compliance, covered entities will have to rely on their data being accurate to determine which activity to report to a degree far beyond current basic risk attribution.

ii. Blockchain analytics firms oftentimes have differing data. If a covered entity relies on the data from one blockchain analytics firm, but a government agency relies on the data from another, a covered entity should not be held liable for misaligned data.

CCI Recommendation: FinCEN should develop and enforce regulatory expectations for blockchain analytics providers as the data required by the NPRM originates from these firms. Before implementing any of the proposed rules, the public and private sectors must collaborate to develop industry standards for blockchain analytics firms to follow. A safe harbor for covered financial institutions should be explicitly included in the rule so they are not held liable for misaligned data received from blockchain analytics firms.

E. With no volume thresholds or any distinctions made between direct and indirect transactions, the NPRM would generate unreasonable incursions into customer privacy as well as enable abuse by malicious actors.

i. As written, the proposed regulations undermine customer data protection, security, and privacy, going beyond analogous regulation of traditional financial institutions.

a. The proposed rule would greatly increase the amount of personal identification information associated with financial transactions to be collected and stored by FinCEN. This increased collection would occur even though the transactions might not be considered suspicious.

b. The increased collection of transactional data by FinCEN heightens the data security risks to consumers, creating honeypots that incentivize bad actors to attempt to breach such troves of information. This makes customers highly vulnerable to cyberhackers and financial scammers who would exploit stolen or leaked data.

c. FinCEN's greater scrutiny on specific wallet addresses–even those not deemed suspicious by financial institutions–could be perceived as increased government surveillance of consumers' past and future transactions indefinitely—far beyond the immediate transaction. This is not possible under traditional banking through wire or automated clearing house (ACH) payments and not expected under the framework of the BSA.

ii. The proposed rules do not sufficiently consider the lawful use of security and privacy tools in the context of blockchain transparency. Under the BSA, consumers must be afforded privacy for legitimate financial transactions. As FinCEN itself acknowledges, "it is reasonable to expect that the relative attractiveness of engaging with CVC mixers or the number of those who avail themselves of CVC mixing services might be affected."[4] As noted, mixing

[4] Proposed Rule at 72716.

services could include commonplace transactions that do not pose the risks that the proposed regulations seek to mitigate.

iii. Without clear guidance on what actually constitutes exposure (such as indirect exposure to a mixer), the current proposed reporting requirements could unfairly implicate innocent users of centralized exchanges. Covered entities should not be required to report customers to FinCEN for all indirect exposure to mixers.

   a. To further elaborate, a customer using a centralized exchange might come into possession of Bitcoin that may have touched a mixing service many transfers ago. Because such mixing contact had nothing to do with the customer, the customer should not be flagged as suspicious or have their personal information reported to FinCEN in a context that unfairly suggests suspicion. If Bitcoin, and other digital assets, can be "tainted" by having ever touched a mixer, there will be undesirable implications for the fungibility of these assets as well as a chilling effect on the use of these assets. It also could create a "guilt by association" for customers who receive too many "flags" and are de-risked, that is far beyond the "drug residue on dollar bills" that would taint innumerable users of fiat currency. In addition, this could lead to data reported to FinCEN becoming meaningless because it would contain vast amounts of legitimate and lawful transactions.

   b. Moreover, while analysis of indirect exposure to mixers may be useful for blockchain investigations, such analysis is unlikely to produce the results that FinCEN expects. It is not effective at conclusively identifying bad actors or high risk transactions without also identifying high volumes of false positives (i.e., transactions that are incorrectly assumed to be related to bad activity). If transactions with indirect exposure to mixers were required to be reported to FinCEN, the effort and cost to report on both bad activity and false positives would be exponential.

iv. As written, the proposed regulations expose customers to malicious activity.

   a. The proposed regulations could expose individuals to dusting. Because indirect transactions could constitute a mixing transaction, a malicious actor could send tiny amounts of low-value tokens to a mixer, back to the malicious actor's wallet, and finally, directly to unsuspecting victims. According to the proposed regulations, the victim's VASP would then have to report their customer and this transaction to FinCEN. Such dusting could be done to complicate the life of the victim and to increase the paperwork burden of VASPs and FinCEN.

CCI Recommendation: Minimize the increase in data collection and storage by FinCEN and prioritize customer privacy by establishing a high volume threshold for reporting mixing services transactions. For example, consider a reporting requirement only for transactions above $10,000, similar to currency transactions reports. Also, FinCEN should narrow reporting requirements to direct exposure to mixers (using the proposed definition in this letter, above) and exclude indirect exposure. Similarly, to safeguard customer data, FinCEN should first establish a secure system to receive from financial institutions the NPRM-required data under the same level of security and protection as provided by the BSA E-Filing System.

F. FinCEN has not provided data and analysis on the usage of lawful privacy-enhancing technologies, making it difficult to assess the economic impact of the NPRM.

i. The rulemaking process would benefit greatly from informed, fact-based discussion about the scope and patterns of mixer use for lawful purposes. Although the NPRM says that "CVC mixing may be used for legitimate purposes," it does not offer much insight into such usage, even though it may be the dominant type of mixer activity. In fact, the NPRM mentions that FinCEN conducted a 2022 study assessing that 33 percent of deposits to a group of CVC mixers came from high-risk sources, which means 67 percent of deposits were not high-risk. But the NPRM's in-depth discussion of mixer data is one-sided, citing only examples of illicit actors exploiting mixers. While this illicit activity deserves attention, for the purpose of rulemaking and assessing the potential impact on consumers and financial institutions, an exploration of both illicit and licit usage is warranted. Imagine a rule that only looked at illicit use of VPNs, without considering the important, legitimate uses – including that the federal government requires employees to use, for security reasons.

CCI Recommendation: FinCEN should conduct a study on lawful and/or low-risk transactions with CVC mixers – with the breadth that the proposed rule defines – and publish the findings in order to inform the public about the full scope of mixing activity. This will allow all stakeholders to better assess potential collateral impacts of such a broad authority with substantial likelihood of chilling development and use of related technology.

G. The NPRM runs the risk of stifling innovation.

i. The digital asset industry is currently developing innovative tools and businesses to promote both privacy and regulatory compliance, including decentralized identity solutions and cryptographic techniques such as zero-knowledge proofs and secure multiparty computation. The White House, in its recent Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, called for the U.S.

to strengthen privacy-preserving technologies.[5] However, the proposed regulation would actually discourage such developments because of the risk that even new tools that support privacy and AML/CFT compliance could be viewed as participating in "mixing services."

a. Under the proposed rule, it is presumed that all mixers are entities that are high risk. Such a presumption fails to acknowledge that it is certainly possible to have mixing services that manage financial integrity risk in both effective and innovative ways. However, under the proposed regulation, FinCEN would be removing the incentive for the development of BSA-level risk-managed privacy-enabling tech.

b. The proposed rule would have a disparate impact on the DeFi ecosystem since DeFi innovations are highly likely to use "programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction." Negatively impacting automated, less intermediated innovation would create an unlevel playing field in the digital asset industry, with smaller ventures facing greater hurdles to innovate and bring new services to market than larger players who are less likely to launch unique or experimental tools. It encourages additional layers of fee-extraction, friction, and vulnerabilities.

c. Please see "Section III" below for a list of innovations currently being developed in the digital asset ecosystem that can help advance both user privacy and AML/CFT risk management around mixing services.

ii. Significant software development is currently occurring to enhance blockchain efficiency and usage. This development could be preempted unfairly if it includes transaction obfuscation designed to improve user experience, not to hide activity.

a. For example, Layer 2 technology protocols, including Lightning or Liquid, could potentially be in scope of the new guidance based on the overly broad definition of a "mixer." Layer 2 protocols are designed to scale an existing Layer 1 blockchain, offer practical utility, and provide increased transaction speed, lower cost and less energy consumption. These technology protocols introduce off-chain methods that occur outside of the transparency of the blockchain, which could be incorrectly perceived to be mixing and thus reportable. However, simply conducting a transaction on a Layer 2 protocol does not automatically mean there is fraudulent activity.

[5] Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (Oct. 30, 2023),https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

CCI Recommendation: FinCEN should host a tech sprint on privacy-preserving compliance solutions, as an area it previously encouraged with a Privacy Enhancing Technology initiative.[6] Also, FinCEN should allow for private sector experimentation through exceptive relief and regulatory sandboxes. This can facilitate the development of crypto-native tools that leverage blockchain technology and transparency to create a compliant ecosystem that effectively combats illicit finance.

H. The NPRM is inconsistent with other jurisdictional regimes and therefore fails to create parity with other regimes. By employing a catch-all approach in the U.S., the NPRM could drive digital asset business activity offshore and negatively impact law enforcement's objectives.

i. In order to develop a workable global framework that effectively mitigates illicit finance, national regulatory schemes must achieve parity. To date, no other jurisdiction has implemented any measures around mixing services similar to what FinCEN is proposing. Thus, the proposed regulations could create a mismatch in regulatory requirements.

ii. AML/CFT rules in jurisdictions should align with the recommendations of the Financial Action Task Force ("FATF").[7]

a. Although the FATF recommendations do not explicitly define the term "mixer," they associate it with other privacy-enhancing technologies such as tumblers and privacy wallets.

b. The FATF recommends that jurisdictions ensure that VASPs effectively manage risks around anonymizing services, but does not call for jurisdictions to collect personal transaction data around mixers. In fact, FATF noted, "[i]t is important to consider any potential implications for privacy and data protection in the use of such tools, if they allow transparency that is not otherwise available (e.g., on public blockchains)."

c. In one example of how jurisdictions have dealt with mixers, FATF highlighted how Japan's Financial Services Agency required VASPs under its jurisdiction to provide the number of customers historically using

[6] *See* FinCEN to Host Innovation Hours Program Workshop on Privacy Enhancing Technologies, available at www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-privacy-enhancing-technologies

[7] *See* FATF Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers, available at https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

mixers or tumblers.[8] This would not have required additional collection of personal transaction data outside of suspicious activity reports.

iii. By ignoring the nuances inherent in different privacy enhancing technologies and proposing reporting requirements that do not align with but also conflict with FATF recommendations, FinCEN would be perpetuating the conflicts between the U.S. and foreign regulations that may ultimately push crypto innovation and activity offshore. This will be detrimental to U.S. law enforcement's efforts to gain information needed to combat financial crime impacting U.S. customers.

CCI Recommendation: FinCEN should seek to align the proposed rules with the recommendations offered by international standard-setting bodies such as FATF and pursue risk-based approaches to privacy-enhancing technologies. FinCEN must take a global approach to ensure a workable regulatory framework for an ultimately borderless technology.

III. Technical Solutions that Reduce the Risk of Illicit Activity with Mixing Services

As further proof that technology continually and quickly evolves, the following are technological tools that the digital assets industry is currently developing to support both privacy and compliance while targeting bad actors.

A. Digital Identity Solutions: As the FinCEN and FDIC digital identity tech sprint[9] illustrated in 2022, entrepreneurs are creating a wide variety of tools to provide third-party proofed and verified digital credentials that users could present for access to online financial services, including digital asset platforms. Solutions can involve a spectrum of approaches, including private institution-managed government-managed, or user-managed.

B. Zero-Knowledge Proofs: Zero-knowledge proofs (ZKPs) are cryptographic tools that allow one party to prove knowledge of certain information without revealing the actual information itself. They can be used to verify the validity of transactions or user credentials without disclosing sensitive data, protecting user privacy while hindering illicit activities. For example, before withdrawing funds from a DeFi service, a digital asset wallet holder could access a ZKP protocol to confirm the wallet address is not on a sanctions list and has not received funds directly or indirectly from a sanctioned address.

[8] *See id.*

[9] *See* FDIC FinCEN Digital Identity Tech Sprint - Key Takeaways and Solution Summaries, available at www.fincen.gov/news/news-releases/fdic-fincen-digital-identity-tech-sprint-key-takeaways-and-solution-summaries

C. Privacy Pools: Privacy Pools[10] are a novel smart contract-based protocol that allows users to demonstrate regulatory compliance by publishing a zero-knowledge proof to show that their funds are not illicit or that they originate from lawful sources–without revealing their entire transaction histories. For example, users could opt-in to have their assets verified through ZKPs in order to be grouped into a pool of non-illicit funds

D. Attestation Tokens/Decentralized Identity: Attestation tokens are cryptographic tools that enable the issuance, verification, and presentation of digital credentials or proofs. These credentials can be used to prove the authenticity of certain attributes or claims without revealing the underlying data. A user who undergoes KYC to verify identity, reputation, or compliance status and receives credentials at a third-party provider could then acquire attestation tokens to transact on a DeFi platform. The tokens' link to a verified identity would reduce the risk of fraudulent activities and illicit fund flows. Decentralized identity tools, in particular, would allow wallet holders to manage their own data and elect when various details are to be revealed for compliance or risk-mitigation needs, thereby providing both verification and protecting data to reveal only the amount needed.

***

IV. Conclusion

CCI supports the goal of preventing illicit finance in the digital assets space. Rules that are precise and clear will be easier for institutions to implement and, thus, will be more effective in stopping financial crime. The most effective way to counter illicit use of mixers is to focus on transactions to or from bad actors.

Blockchain-based applications, including privacy-enhancing technologies, have already delivered and promise to continue to bring great benefits to consumers, investors, and the economy as a whole. Thus, policymakers should refrain from arbitrarily limiting the use of mixers, either directly by prohibition or indirectly by imposing unnecessary and burdensome regulatory requirements upon service providers.

As FinCEN considers how to promote responsible innovation with respect to mixers, we respectfully encourage the agency to consider the recommendations we have laid out in this letter. We look forward to further working with FINCEN on how covered financial institutions can comply with these reporting requirements in light of the broad applications and use cases

[10] *See* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364

that could be captured. CCI is fully aligned with the aim of mitigating money laundering and illicit activity across all areas of financial services, and we hope to be a resource to FinCEN and work together in developing a proposal that best achieves that goal.

Respectfully submitted,

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation

Ji Hun Kim
General Counsel & Head of Global Policy
Crypto Council for Innovation

Yaya J. Fanusie
Director of Policy for AML & Cyber Risk
Crypto Council for Innovation