January 22, 2024

Response to FinCEN's Notice of Proposed Rulemaking on CVC Mixing as a Class of Transactions of Primary Money Laundering Concern (Docket No. FINCEN-2023-0016) By Polygon Labs and DELV

Introduction

Polygon Labs and DELV (formerly known as Element Finance, Inc.) respectfully submit this response (the "Response") to the request for comments on the notice of proposed rulemaking published by the Financial Crimes Enforcement Network ("FinCEN") entitled "Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class Of Transactions of Primary Money Laundering Concern," published October 23, 2023 (the "NPRM").[1]

Polygon Labs and DELV share FinCEN's goals of detecting and deterring "illicit activities" – namely, "money laundering and other financial crimes"[2] – in blockchain technology. As discussed further below, however, the proposed definition of "CVC mixing" in the NPRM (the "Proposed Mixing Definition") is unreasonably broad – so much so that the "additional recordkeeping and reporting requirements" imposed on "covered financial institutions," including money services businesses ("MSBs") and other virtual asset service providers ("VASPs") that interact with CVC mixing "within or involving a jurisdiction outside the United States" (the "Proposed Rule") would be so burdensome as to – in effect – discourage nearly *all* use of blockchain technology by these centralized, BSA-obligated entities. Cutting off U.S. financial institutions from this technology will negatively impact U.S. national security and economic prosperity; it will curtail, not enhance, U.S. law enforcement's visibility into illicit use of CVC mixing activity.

This Response is structured as follows: Section I provides a brief background of the relevant technology that may be captured inadvertently by the Proposed Mixing Definition – notably, centralized and decentralized mixers, decentralized finance ("DeFi") protocols, bridges, and zk technology (for purposes of this paper only, the "Relevant Technology"); it also discusses the way that "covered financial institutions" may interact with the Relevant Technology. Section II

[1] Polygon Labs is an international software development company that builds blockchain infrastructure and complementary software, with a mission to provide more efficient and open blockchain infrastructure on which third party developers and the global community can build. DELV (f/k/a Element Finance, Inc.) is a research and development studio dedicated to advancing the safe adoption of decentralized financial systems by building a suite of novel, research-backed, and open source software infrastructure.

[2] NPRM at 72713.

analyzes a number of issues raised by the Rule – notably, the overbreadth of the Proposed Mixing Definition, how the Rule is a departure from FinCEN's previous Section 311 approaches, and how the Rule, in practice, amounts to a special measure five. Section III further addresses the "legitimate business purposes" for not only CVC Mixing, but also other technology captured by the Proposed Mixing Definition – and how the NPRM ignores the statutory mandate to properly consider these legitimate business purposes. Section IV lays out how the Proposed Rule is administratively impracticable: both because the technology makes it impossible for a "covered financial institution" (or anyone except the user) to determine whether a transaction occurred "within or involving a jurisdiction outside the United States" while creating duplicative processes that are in tension with other anti-money laundering ("AML") requirements set forth by the Bank Secrecy Act ("BSA"). Critically, this Section also sets forth how the Proposed Rule – if implemented – will hamper U.S. national security interests, especially as it relates to law enforcement's ability to detect and deter illicit activity using CVC mixers. Finally, Section V proposes an alternative path forward to accomplish the policy goals underlying the Proposed Rule.

We thank FinCEN for its consideration of the matters raised in this Response, and would be happy to discuss these at the agency's convenience.

I. Overview of Certain Blockchain Technology Relevant to The Response

The Proposed Mixing Definition seeks to capture certain blockchain technology that purportedly "obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used."[3] To narrow this admittedly "broad" description, FinCEN enumerates a number of types of "protocols or services" that may meet the Proposed Mixing Definition, including – and, most relevant for the Response – "(1) pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts; (2) using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction . . . ."[4]

Certain software code is intentionally built to protect the privacy of user transactions so that they are not traceable and/or that data relating to user transactions is not available; in other words, the code allows users to shield their transaction information from the inherent transparency of public blockchains. The first two enumerated examples in the Proposed Mixing Definition are so broad, however, that they may capture a significant portion of blockchain technology – including technology where data remains available to meet the policy goals underlying the Proposed Rule – namely, to "collect information, which will discourage the use of CVC mixing by illicit actors,

[3] NPRM at 72709.
[4] *Ibid*.

and is necessary to better understand the illicit finance risk posed by CVC mixing and investigate those who seek to use CVC mixing for illicit ends."[5]

A. Relevant Blockchain Technology.

Although transactions involving CVC mixers comprise a small portion of the total transactions in the larger blockchain ecosystem, the Proposed Mixing Definition is so broad that it captures some of the most critical blockchain technology today – technology core to how users are scaling blockchain networks, to the interoperability of blockchain networks, and to some of the most novel applications built upon blockchain networks.

1. *Mixers*

There are two types of CVC "mixers" – centralized and decentralized. FinCEN's guidance issued in 2019 entitled "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" sets forth the distinction between the two: "mixers" are "either persons that accept CVCs and retransmit them in a manner designed to prevent others from tracing the transmission back to its source (anonymizing services provider), or suppliers of software a transmittor would use for the same purpose (anonymizing software provider)."[6] The former may be referred to as "centralized" mixers and the latter software developed by the "suppliers" referenced in the 2019 Guidance, "decentralized mixers."

Centralized mixers are those run by a "person" (as defined by FinCEN's regulations) who accepts CVC from a user and then sends the CVC to the same user, but with a different destination than the sending address. Typically users send CVC to centralized mixers through another type of software called a "wallet," which is code comprising two unique numbers, each called keys: one public key, which is an identifier that lets users receive cryptocurrencies – similar to an email address – and one private key, which allows the user to access and send the cryptocurrencies associated with the paired public key – similar to a password. A centralized mixer is custodial – the person (i.e., intermediary) takes possession of a customer's CVC. These types of mixers may also be called "permissioned" because they are run by intermediaries. Custodial, centralized mixers function as money service businesses.

Decentralized, non-custodial, permissionless mixing services remove these intermediaries by replacing them with software called "smart contracts" (defined below) that allow users to supply CVC to a software protocol – a set of rules set by the code – through one self-hosted wallet and then allow the same user to withdraw their CVC using any wallet (whether the same as the

[5] NPRM at 72706.
[6] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019) ("2019 Guidance") at 19, *available at* https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

depositing one or a different one). Users are able to withdraw CVC to a second (or same) wallet by holding a "deposit note," a proof as generated by zk proofs (defined below) built into the smart contract. The deposit note is a receipt which allows the user to prove that they supplied a certain amount of CVC through the first wallet. Technically, the deposit note is generated and stored locally on a user's own computer and only the encoded form – the hash – of the note is added to the public list of all the users' encoded notes on the underlying blockchain.

When a user wants to withdraw CVC, the user will initiate a withdrawal from the smart contract. To do so, the user will supply the hash and the deposit note to the smart contract to verify: (a) the CVC being withdrawn were previously deposited into the smart contract, (b) the user is holding a note relating to CVC supplied to the smart contracts, and (c) the CVC being withdrawn were not previously withdrawn. Upon verification, the user will be able to receive the CVC to their original or second wallet.

Decentralized mixers are part of a broader software system known as "decentralized finance," which we discuss below.

2. *Decentralized Finance ("DeFi")*

DeFi protocols are technological systems (a) comprised of software known as "smart contracts," (b) in which users can engage in economic transactions in a self-directed manner, (c) without a need for an intermediary, (d) where no person or entity takes custody of a user's assets, and (e) where all elements of transactions occur on a permissionless blockchain network.

Smart contracts are self-executing computer programs – software code – that function in a conditional manner (*i.e.*, "if X, then Y"). Smart contracts that function together in a complementary way and speak to each other based upon a user's directions are referred to as a "protocol" – a set of rules defined in code that govern how economic transactions can occur. These smart contracts governing DeFi protocols have two key characteristics: first, they are autonomous, in that they execute without an intermediary and are automatic (i.e., execute so long as the underlying conditions are met); second, they are composable, in that they are able to be combined and used like building blocks to create a number of different use cases. Many DeFi protocols function through smart contracts that "pool" CVC to allow for users to engage in various economic transactions.

For example, an automated market maker[7] – a type of decentralized exchange – is comprised of "liquidity pools" that allow users to supply two different tokens to the pool in a way that (1) sets

[7] AMMs are the most widely used across all DEXs. Therefore, in this response "AMM" will be used interchangeably with "DEX", although not all DEXs use AMMs. *See* https://coinmarketcap.com/academy/article/3-minute-tips-the-different-types-of-decentralized-exchange-dex

the price of the tokens through an automatic mechanism,[8] which updates the price of the tokens every time there is a change in the ratio of the tokens in the pool, and (2) allows users to exchange tokens through the pool. To use these pools for trading, a user would send one token (CVC A) plus the associated fee to the pool's smart contracts, and in return, would receive the other token (CVC B).

Similarly, liquidity provision protocols – colloquially referred to as "lending protocols" – allow users to send one type of CVC to a "pool" and then borrow – in an over-collateralized manner – against the amount of the CVC sent from another "pool." In a typical transaction, a user may supply $150 worth of USD Coin ("USDC"), a fiat-backed stablecoin, to a smart contract pool of USDC; the user will receive a receipt – typically another type of CVC – in their wallet which documents the supplied USDC; then the user may borrow $100 worth of another type of CVC, also held in a larger "pool" – for example, $100 worth of Ethereum ("ETH") from a larger pool of ETH, which has been supplied by other users. The smart contracts in the protocol will "read" the user's receipt – held in their wallet – and allow the user to borrow against the supplied CVC.

Other types of DeFi protocols function through a similar mechanism in which smart contracts create pools of tokens that can be used for different purposes (such as borrowing as described in the example above).

DeFi protocols were not created to "obfuscate[ ] the source, destination, or amount involved in one or more transactions".[9] However, it is possible that, because of the way DeFi protocols function, it may not be possible to trace the source, destination or amount involved in certain DeFi transactions. This may be particularly true where a DeFi protocol has been deployed to a permissionless blockchain enabled through zero knowledge ("zk") technology (discussed below). Regardless, all *true* DeFi transactions are user-directed, without an intermediary that takes custody.

Further, DeFi transactions on permissionless blockchain networks do not allow for tracing or tracking certain information – namely, and as relevant to this Response – the *location* from which the user originated or received a transaction. As noted above, users initiate transactions on permissionless blockchain networks through software known as self-hosted wallets. These wallets are identified as a string of letters and numbers which do not contain any specific identifying information about the user – *i.e.*, wallets are pseudonymous. The wallet itself can be traced through a block explorer (a website tracking all transactions on a blockchain network), but

[8] *See*, https://collectiveshift.io/defi/amm-guide/. ("The most popular is the 'constant product market maker' mechanism—often called the 'constant function market maker' ('CFMM')—that has the simplified formula, x*y=k, where 'x' and 'y' are the reserves of each asset. The term 'constant function' refers to the fact that any trade must change the reserves in such a way that the product of those reserves remains unchanged (i.e. equal to a constant).")

[9] NPRM, *supra* note 3.

nothing else about who owns or uses the wallet can be traced – not their name (unless associated with a special blockchain-based identifier through the Ethereum Naming System), their location, etc.

3. *Bridges*

One of the more recent challenges in blockchain technology concerns interoperability across blockchain networks. In other words, networks often do not automatically communicate and share data – including information about CVC – across different blockchains. Bridges make this communication and data sharing possible.

A "bridge" is software code that allows users to create a representation of a cryptocurrency relating one blockchain to another. Users supply CVC on one blockchain and then cause the bridge – through its code – to send a message to smart contracts on another blockchain. That message then "mints" – or creates a representation of – another CVC (sometimes referred to as a "wrapped asset") in the same amount on the other blockchain. This creates a new CVC on the second blockchain with its value pegged to the original CVC.[10] The CVC on the original blockchain is supplied by the user to the bridge protocol where they remain, such that the "wrapped asset" is the only CVC that can be moved on-chain.

Although there are different types of bridges, they typically function in the following way: first, a user supplies CVC A in a smart contract on blockchain A. The smart contract then issues ("mints") a new CVC – "wrapped asset" B – on blockchain B and sends this "wrapped asset" to the same user on blockchain B. To move back to blockchain A, the user supplies "wrapped asset" B in a smart contract on blockchain B. The smart contract then "burns" (or destroys) the "wrapped asset" B on blockchain B, "unlocks" CVC A on blockchain A, and returns CVC A to the user's self-hosted wallet on blockchain A.

Bridges are relevant to the Proposed Mixing Definition because the bridge smart contracts "pool" CVC as part of the "wrapping" process on one blockchain to communicate the value relating to that CVC to another blockchain. As such, bridges might be deemed CVC mixing under definition (3)(A) of the Proposed Rule.[11]

4. *Zero knowledge ("zk") proofs*

Zero knowledge proofs ("zk proofs" or "ZKPs") are cryptographic tools that allow one party (the "prover") to prove a piece of information to another party (the "verifier") without revealing anything about the information itself. Zk proofs have become a core architecture component of

[10] For more on bridges, *see* https://chain.link/education-hub/cross-chain-bridge.
[11] NPRM at 72722 ("Pooling or aggregating CVC from multiple persons, wallets, addresses or accounts").

many blockchain scaling solutions, also called layer 2 networks or L2s. L2s are designed to increase the speed and reduce the cost[12] of validating transactions on a layer 1 ("L1") blockchain – like Ethereum – by batching many transactions together into a single one, reducing the computational load of the L1[13] (i.e., L1 only needs to validate one, batched transaction versus all the individual transactions included in the batch). ZKPs allow L2s to further reduce this computational load by providing a *proof* of the batched transactions, which is computationally easier to validate than the batches of transactions.

In L2 networks, the L2 functions as the prover and the L1 as the verifier, with the L2 having to generate and supply proof to the L1 that the batched transactions are valid. To generate this proof, the L2 uses a proving mechanism that – through complex algorithms like polynomials[14] and elliptic curve pairs[15] – takes in some input (i.e., transaction details of the batched L2 transactions) and produces an output (i.e., the ZKP). The L2 will then send this ZKP to the L1, which will validate the *proof* – instead of the batched transaction or individual transactions – before adding the batched transaction to the underlying ledger. ZKPs are programmatic and/or algorithmic code that ultimately coordinate the structure of transactions on some L2s.

On L1 networks, all transaction data – including wallet addresses, transaction amounts, times of transaction, etc. – is recorded on the blockchain ledger, giving L1 networks their transparency. ZKPs do not provide this level of transparency because a ZKP is a *proof* of transactions; therefore, it does not include any of the transaction details like those recorded on L1 networks. Instead, the ZKP includes transaction hashes – strings of letters and numbers that serve as unique identifiers for each transaction). Transaction details – like sending wallet address, receiving wallet address, and amounts transacted – are used in generating the ZKP but are not recorded in the same ways as L1 transactions to give users a layer of privacy.[16]

Generally, L2s must make the data associated with each individual transaction available and accessible to other network participants (referred to as "data availability") to provide sufficient assurance that the transactions in a given batch were verified correctly (i.e., in accordance with the rules of the network). With ZKPs, L2s can conceal transaction data at the L2 level (i.e., the

[12] For example, as of January 3, 2024, on the Polygon POS network, another L2 on Ethereum developed by Polygon Labs, a transaction takes 2.2 seconds to verify and costs less than $0.01. *See* https://polygonscan.com/.; In contrast, on the Ethereum network, a transaction takes 12 seconds to verify and costs $2.24. *See* https://etherscan.io/ and https://etherscan.io/chart/blocktime.

[13] Figure 2 demonstrates how the L1 can only "fit" five transactions into a block to verify. When an L2 is involved, it is able to "fit" nine transactions into a block. If each block takes the same computational power to verify, then an L2 allows an L1 to validate more transactions with the same amount of computational power, meaning less computational power required per individual transaction. In practice, L2s are able to batch thousands of transactions for L1s.

[14] *See* Eli Ben-Sasson, Iddo Bentov, Yinon Horesh & Michael Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," Cornell University (Mar. 6, 2018), *available at:* https://eprint.iacr.org/2018/046.

[15] *See* Thomas Chen, Hui Lu, Teeramet Kunpittaya & Alan Luo, "A Review of zk-SNARKs," Cornell University (Oct. 25, 2023), available at: https://arxiv.org/abs/2202.06877

[16] *See e.g.*, https://nakamoto.com/zcash-the-https-of-blockchains/

L1 cannot "see" the details of any individual transactions included in an L2 batch, meaning these details do not show up on block explorers) by using tactics like data encryption.[17] However, this does not mean that the data is inaccessible; instead, the data can be made available or accessed in other ways. For example, users maintain control over their financial data and can make it accessible to trusted third parties.[18]

B. The Way In Which "VASPs" Interact With the Relevant Technology.

Financial institutions in the crypto space – typically MSBs that are operating as exchanges, centralized stablecoin issuers or over-the-counter trading desks, among others – relate to and/or interact with much of the Relevant Technology on a frequent basis today. Although the NPRM uses the term "VASP" – "virtual asset service provider" – somewhat interchangeably to refer to "covered financial institutions" as defined by 31 C.F.R. § 1010.100(t) and "money services businesses" as defined by 31 C.F.R. § 1010.100(ff),[19] we are not aware of any specific law, regulation or rule in the United States that defines – or leverages – the term VASP.[20]

To the extent that we use the term "VASP" in the Response, it has the same meaning as set forth by the Financial Action Task Force ("FATF"):

> "Virtual asset service provider means any *natural or legal person* who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
>
> i. exchange between virtual assets and fiat currencies;
>
> ii. exchange between one or more forms of virtual assets;
>
> iii. transfer of virtual assets;
>
> iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
>
> v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."[21]

[17] *See e.g.*, https://learn.bybit.com/altcoins/what-is-zcash-zec/
[18] *Ibid*.
[19] NPRM at 72709-10.
[20] We recognize that FinCEN used the term "VASP" in its imposition of special measures against a CVC exchanger, Bitzlato Limited. *See* FinCEN, "Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitzlato" (Feb. 1, 2023).
[21] FATF, "12 Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 2020), Annex A, *available at* https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (emphasis supplied).

Regardless of the term used, these centralized, off-chain entities – most of which are registered as MSBs in the U.S. – interact with the Relevant Technology regularly.

Although much of the focus on VASPs relates to how users "on- and off-ramp" from the traditional, fiat-based economic system – that users convert CVC to and from fiat currency using these entities – VASPs are integrated in a variety of ways with the Relevant Technology. VASPs may integrate with or otherwise interact with bridges, L2s and DeFi in order to allow users to engage in various types of activities, including but not limited to transferring the representation of CVC value from one blockchain network to another, among other things. Further, the Proposed Rule does not specify whether "a CVC transaction involv[ing] the use of CVC mixing" must be the transaction immediately preceding a user's "off-ramping" transaction with the VASP (the "Final Transaction") or *anywhere* in the chain of transactions prior to the transaction with the VASP – multiple "hops" prior to the Final Transaction; without such a limitation on the proximity of a CVC mixing transaction to a Final Transaction, nearly all Final Transactions will have had some interaction with some type of the Relevant Technology.

II. Analysis of the Rule

A. The Definition of CVC Mixing Activity Is Overbroad.

As noted above, the Proposed Mixing Definition is most problematic – in regards to the Relevant Technology – with respect to the first two limiting prongs of "facilitati[ng] 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": "(A) [p]ooling or aggregating CVC from multiple persons, wallets, addresses, or accounts; (B) [u]sing programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction . . . ."

First, the initial prong of "pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts" would capture most if not all of DeFi applications and bridges. Although much of DeFi and bridges do not intentionally "obfuscate[] the source, destination or amount involved in one or more transactions," by pooling CVC, certain information on "source, destination, or amount" may not be as readily available or transparent as sought by the Proposed Rule, even if the data about the transaction is ultimately available. Although smart contracts in DeFi and bridges may combine user funds, they were not designed to do so with the purpose or intent of "obfuscating the identity of both parties to the transaction by decreasing the probability of determining both intended persons for each unique transaction."[22] These smart contracts only pool user funds so the protocols can bring about various benefits – including lack of counterparty

[22] NRPM at 72703.

risk and greater efficiency in financial transactions – that otherwise do not exist in traditional, intermediary-based transactions.

Second, the second prong – "using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction" – would capture zk-enabled L2 blockchains and the applications built on top of them, even if the applications themselves do not use zk proofs. As described, zk technology uses code – specifically, code that uses complex mathematical functions – to "coordinate[] two or more persons' transactions together" but *not* in order to "obfuscate the individual unique transactions by providing multiple potential outputs from a coordinated input, decreasing the probability of determining both intended persons for each unique transaction."[23] Zk technology, "coordinates" transactions insofar as verifying them and generating a proof that the transactions are valid. Moreover, even if the code does "coordinate" these transactions – which may "obfuscate" certain information about individual transactions – it does so only from the perspective of the verifier. L2 networks must make transaction data available to other network participants to ensure that the transactions are being verified according to the rules of the network. Without making this data available, L2 networks cannot function because no one can validate if the L2 network's batched transactions are correct. The "data availability" feature of L2s means that the code does not *actually* "obfuscate" transaction information, even if it is not transparent in the same way as L1 transaction data.

The Proposed Mixing Definition thus captures technology that otherwise has *not* necessarily been found to be "of primary money laundering concern." There is no discussion in the NPRM relating to zk technology, bridges, or DeFi – let alone a finding that any of this technology may fall under the appropriate designation to warrant any special measures under Section 311. As a corollary – and as discussed further below – and as discussed further below there is no discussion or consideration of the legitimate uses of these technologies, as required by the statute. Given the breadth of the language throughout the definition of "CVC mixing," such technologies will be subject to the enhanced recordkeeping and reporting requirements set forth by the Proposed Rule.

B. The NPRM is an Unwarranted Departure from FinCEN's Previous Section 311 Approaches, Which Were Targeted and Tailored in Response to a Specific Threat.

Since the passage of the USA PATRIOT Act twenty-two years ago, FinCEN has used the Section 311 authority – an "important and extraordinarily powerful tool"[24] – only twenty-three times, with only eleven proposed rules becoming final. The U.S. Treasury Department ("Treasury")

[23] *Ibid*.
[24] Testimony before the Senate Committee on Finance, under Secretary for Terrorism and Financial Intelligence Stuart Levey (April 1, 2008) at 15, *available at:* https://www.finance.senate.gov/imo/media/doc/040108sltest.pdf.

describes Section 311 as one that "provides the Secretary with a range of options that can be adapted to target specific money laundering and terrorist financing risks most effectively."[25]

In 2008, then-Under Secretary Levey of the U.S. Department of the Treasury explained how the Section 311 authority, using measures to "finely-target" a specific concern, can be incredibly effective:

> "In the case of broad, country-wide sanctions that are often perceived as political statements, it can be difficult to persuade other governments and private businesses to join us in taking action. Even when other governments agree with us politically, they generally tend to be unwilling to force their businesses to forgo opportunities that remain open to others. When the private sector views such broad sanctions as unwelcome barriers to business, companies are unmotivated to do more than what is minimally necessary to comply. Indeed, history is replete with examples of participants in the global economy working to evade such sanctions while their governments turn a blind eye.
>
> * * * * *
>
> The key difference when we use targeted financial measures is the reaction of the private sector. Rather than grudgingly complying with, or even trying to evade these measures, we have seen many members of the banking industry, in particular, voluntarily go beyond their legal requirements because they do not want to handle illicit business. This is a product of good corporate citizenship and a desire to protect their institutions' reputations. The end result is that private sector voluntary actions amplify the effectiveness of government-imposed measures."[26]

Prior to the Proposed Rule, FinCEN has exercised this targeted authority under Section 311 in relation to specific entities, such as foreign banks or exchange houses, or to specific jurisdictions, such as the Islamic Republic of Iran, the Democratic People's Republic of Korea, or the Republic of Nauru. FinCEN has also effectively used this targeted Section 311 authority – and its counterpart, the 9714 Special Measures authority pursuant to the Combating Russian Money Laundering Act[27] – against various crypto-related entities and threats.[28] This is consistent with

---

[25] U.S. Department of the Treasury, *Fact Sheet: Overview of Section 3111 of the USA PATRIOT Act*, (February 11, 2011), *available at:* https://home.treasury.gov/news/press-releases/tg1056.
[26] Testimony before the Senate Committee on Finance, under Secretary for Terrorism and Financial Intelligence Stuart Levey, at 2-3 (April 1, 2008), *available at:* https://www.finance.senate.gov/imo/media/doc/040108sltest.pdf.
[27] *See* Combating Russian Money Laundering Act, Section 9714 of the NDAA.
[28] *See, e.g.*, Section 9714 action against Bitzlato (January 2023), *available at*: https://www.fincen.gov/sites/default/files/shared/Order_Bitzlato_FINAL%20508.pdf; See also Section 311 action regarding Liberty Reserve, S.A. (May 2013), available at: https://www.fincen.gov/sites/default/files/shared/311--LR-NPRM-Final.pdf.

the Treasury's acknowledgement that this powerful statutory authority is exceptional and to be used in a narrow, targeted way to effect its purposes.[29]

As FinCEN recognized[30] in the NPRM, the Proposed Rule marks the first effort to categorize a "class of transactions" as an area of "primary money laundering concern" within the meaning of Section 311. The novelty, of course, is not problematic: it is entirely possible to appropriately designate a "class of transactions" as of primary money laundering concern, and then impose one or more of the five special measures to specifically target that concern. Indeed, Section 5318A envisions just that: a predicate finding that a certain specific, targeted class of transactions – or type of account, jurisdiction, or institution – constitutes a primary money laundering concern, warranting the exceptional measures in a Section 311 rule.

Unlike FinCEN's prior Section 311 and 9714 designations, the Proposed Rule does not use a targeted approach, and therefore, invites a host of problems relating to compliance, enlisting international cooperation, and remaining consistent with the purposes of the statute. By covering nearly all blockchain technology (*see* Part II.A), the broad-brush approach misses the focus on real potential threats caused by mixers and other obscuring technology by bad actors. It would also, contrary to the aims of Section 311 itself, create significant competitive disadvantages to U.S.-based covered entities, and adversely affect legitimate business activities for legitimate mixing activities.[31]

To be clear, however, we do not suggest that the government ignore the threats posed by CVC mixers and perhaps even some activities which might be considered "mixing activity." Rather, as invited by the questions in the NPRM, we respectfully submit that a specific, targeted response would better serve the government's interests and would avoid many of the adverse consequences of the current Proposed Rule as drafted. Such an approach would also focus more accurately on the precise national security, economic, and illicit finance issues highlighted in the NPRM findings.

C. The Proposed Rule, As Drafted, is Tantamount to a Special Measure Five.

The overly broad definition of CVC Mixing would likely result in one of three approaches by a covered financial institution: (1) apply the Proposed Rule to *all* transactions potentially involving

[29] Treasury has described the use of the Section 311 authority as a "strategy of using targeted, conduct-based financial measures aimed at particular bad actors." See Testimony before the Senate Committee on Finance, under Secretary for Terrorism and Financial Intelligence Stuart Levey (April 1, 2008), quoted in GAO Report GAO-08-1058, "USA PATRIOT ACT: Better Interagency Coordination and Implementing Guidance for Section 311 Could Improve U.S. Anti-Money Laundering Efforts," September 2008, p.26, *available at*: https://www.gao.gov/assets/gao-08-1058.pdf.
[30] FinCEN, "FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing" (October 19, 2023), *available at* https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency.
[31] See 31 U.S.C. 5318A(a)(4)(B)(ii) and (iii).

CVC Mixing (per the Proposed Mixing Definition); (2) apply the Proposed Rule to *none* of the transactions involving CVC Mixing; or (3) refuse to process any transactions otherwise where it "knows, suspects, or has reason to suspect involves" CVC Mixing. In order to comply with relevant obligations, covered financial institutions undoubtedly default to either the first or the third approach. In the event a covered financial institution continues to allow and/or process transactions that it "knows, suspects, or has reason to suspect involves" CVC Mixing and applies the enhanced requirements to *all* such transactions (option 1), the covered financial institution will be applying such requirements to nearly *all* blockchain transactions, given that the Proposed Mixing Definition encompasses L2s, bridges, and DeFi. For these reasons, the Proposed Rule is administratively impracticable (discussed below) as covered financial institutions will be required to engage in enhanced recordkeeping and reporting on almost *all* transactions under the requirements of the Proposed Rule.

In fact, the NPRM recognizes that the third option may be the more likely outcome: "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."[32] Therefore, instead of "maintain[ing] records, fil[ing] reports, or both" – as is consistent with the aims of special measure one – the effect of the Rule would instead indirectly "prohibit" U.S. financial institutions from interacting with any parts of the technology – tantamount to the effects of special measure five.

III. There Are Legitimate Business Purposes For the Relevant Technology.

A. The NPRM Ignores the Statutory Mandate to Consider Legitimate Uses of Mixers.

The statutory framework requires that Treasury must make a number of inter-agency consultations before selecting which special measure to impose, and "shall consider" various factors, including, among other things, the extent to which a proposed action might have a "significant adverse systemic impact" on "legitimate business activities" regarding the Section 311 target.[33] In other words, prior to selecting one or more special measures, FinCEN must affirmatively assess the amount and extent of current, legitimate CVC mixing activity, as well as the adverse effect of the Proposed Rule upon such legitimate activity.

The Proposed Rule fails to do this. In the NPRM, FinCEN acknowledges that "there are legitimate reasons why responsible actors might want to conduct financial transactions in a secure and private manner given the amount of information available on public blockchains."[34] It

[32] NPRM at 72716.
[33] 31 U.S.C. 5318A(c)(2).
[34] NPRM 72706.

further recognizes that CVC mixing activity has other licit uses, "such as privacy enhancement for those who live under repressive regimes or wish to conduct licit transactions anonymously."[35] Thus, FinCEN fully – and appropriately – recognizes the need for a balance to ensure that legitimate uses are protected.

But the balance – and even the necessary consideration required under the statute – never occurs in the NPRM. FinCEN states that it cannot assess the extent or volume of legitimate activity, and so it states – in an *ipse dixit* manner and without adequate support – that the "substantial risks of CVC mixing" for illicit finance warrants its proposed remedy. Despite not knowing the extent or volume of legitimate use, FinCEN assesses that the Proposed Rule "would have minimal impact upon the international payment, clearance and settlement system, or on legitimate business activities involving CVC transactions."[36] That the NPRM affirmatively seeks responses and information about legitimate business uses for CVC mixing activity in itself proves the point: FinCEN does not have significant or even sufficient information to make a determination about the balancing of the burdens imposed by the Proposed Rule against the benefits of the legitimate business use. That flaw notwithstanding, the NPRM concludes that the Proposed Rule addresses and mitigates illicit finance risks "while preserving legitimate actors' ability to continue conducting secure and private financial transactions."[37]

The NPRM further acknowledges that this calculus cannot be made by financial institutions, either. In opining whether a Section 311 action might be tailored to address the actual risks outlined in the factual findings – such as the use by North Korea-sponsored actors, Hamas, or the Palestinian Islamic Jihad – FinCEN notes that "covered financial institutions would typically have insufficient information to determine" whether such transactions had this nexus. Thus, in evaluating the impact of the rule, FinCEN concedes that it would reverse the presumption: "The reporting and recordkeeping requirements under special measure one would instead guide a covered financial institution to presume transactions that involve CVC mixing are inherently of primary money laundering concern.

Therefore, under this proposal, the implied burden would shift from determining when a CVC transaction is reportable to determining when it is not reportable";[38] and because there are serious consequences for failing to report a reportable transaction, but no consequences to reporting a legitimate transaction, it is extremely likely that *all* mixing transactions would be reported, or, as discussed herein, covered financial institutions would not process or otherwise interact with transactions that involved CVC mixing rather than take on the enormous additional compliance

[35] *Ibid*.
[36] NPRM at 72708.
[37] NPRM at 72709.
[38] NPRM at 72713 (emphasis added).

burdens and enforcement exposure. As noted above in Section II.C, this would make the regulatory action tantamount to special measure five.

B. There are Significant Legitimate Business Purposes For the Relevant Technology.

1. *Mixers*

As FinCEN notes, "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."[39] Privacy – especially financial privacy – is widely accepted as necessary in the U.S., for a number of reasons. Many of these reasons are to avoid negative consequences (e.g., punishment from an authoritarian government, physical targeting by malicious actors, and business disadvantages and potential extortion from competitors – as discussed further below). Below we provide legitimate business uses for CVC mixing, as requested in the NPRM.

Donation anonymity. Individuals can use mixers to make anonymous donations or contributions to politicians, charities, and causes they care about without fear of negative repercussions, which can range from judgment from peers to government persecution to avoiding inappropriate demands for additional donations. Mixers also give users religious privacy with tithes and other forms of faith-focused payments or donations. In addition to privacy for donors, mixers also afford the recipients of donations privacy, since there could be a spotlight put on organizations that receive funding from certain individuals.

A recent example of this mixer use case was the wave of donations to the Ukrainian government following Russia's invasion.[40] Vitalik Buterin, Russian-born co-founder of Ethereum, publicly stated[41] that he used privacy preserving tools to facilitate his donations to Ukraine. For such a circumstance, donating to the Ukrainian government, through a mixer, allowed individuals to conceal their support of Ukraine from the Russian government, protecting themselves from surveillance by a repressive regime.

Harm reduction. High net worth individuals, public figures, whistleblowers, and others may want to use mixers to conceal their money from and avoid being targeted by malicious individuals who seek to rob, kidnap, or inflict physical, emotional, or reputational harm on them. Even in traditional financial systems, if an individual's financial data is protected, they are less vulnerable to scams, phishing, extortion, or in the most extreme cases physical harm.

---

[39] NPRM at 72702.
[40] *See e.g.*, "Crypto and Ukraine - Fundraising at Speed," Crypto Council for Innovation (Oct. 23), *available at:* https://cryptoforinnovation.org/crypto-case-study-ukraine/
[41] *See* https://twitter.com/VitalikButerin/status/1556925602233569280

Financial protection. Public figures may want to use mixers to shield their financial activity from their followers – i.e., preventing their followers from taking their personal financial activities as financial advice and replicating them. For example, a well-known developer may want to test certain software that they do not want people to interact with because they may lose money. With a mixer, the developer can do this without inadvertently putting their followers at risk.

Business operations. Companies may carry out business deals on the blockchain, while protecting trade secrets or private business matters by concealing – primarily from competitors – who they are paying, how much they are paying, and potentially what they are paying for. In addition, businesses may use mixers as part of the payroll process, so employees can receive their paychecks in a way that prevents them from being poached by competitors and does not expose their personal finances to their coworkers.

2. *DeFi*

Separate and apart from the legitimate use cases for mixers, there are significant benefits to DeFi that must be considered if FinCEN intends to implement the Proposed Mixing Definition, which, as noted above, includes DeFi.

Efficiency. Autonomous smart contracts enable near-instant and atomic settlement of transactions. In addition, they function as "checks and balances" of the transaction; if any part of the smart contract rules is not met during the transaction process, the transaction will not be carried out. Composable[42] smart contracts enable multiple actions to be carried at once, creating efficiencies in financial transactions that do not otherwise exist in the traditional financial sector, allowing for decreased costs[43] associated with executing a transaction, increased speed[44] of transaction execution, and new ways of transacting and sharing value online.[45]

Transparency. In addition, the underlying code for true DeFi protocols is transparent, open and accessible – anyone with a computer and Internet connection can view all parts of the code at any time – contrasted against the opacity of traditional systems. The transparency allows users to know exactly what will happen at every point of the transaction lifecycle before ever initiating a

[42] *See e.g.,* https://ethereum.org/developers/docs/smart-contracts/composability
[43] In 2022, The World Bank found that the price of sending remittances was around 6.3% for sending $200. *See* https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q322_final.pdf; Alternatively, sending a transaction – no matter the amount or destination – on a blockchain like Ethereum costs $0.78. *See* https://etherscan.io/; Moreover, using L2 solutions could further bring down transaction costs to less than a penny. *See e.g.*, https://coinwire.com/cheapest-crypto-to-transfer/.
[44] For example, international transfers could take anywhere between one to five business days. *See e.g.*, https://www.westernunion.com/blog/en/us-how-long-does-money-transfer-take/; In contrast, transactions on a blockchain take anywhere from a few seconds to minutes and can happen 24/7/365. *See e.g.*, https://coinwire.com/cheapest-crypto-to-transfer/.
[45] For a database of these use cases – such as volatility hedge, emergency aid disbursement, crowdfunding, to name a few – *see* https://thevalueprop.io/database.

transaction, removing information asymmetries, counterparty risks, and risks borne from errors in human or subjective judgment[46] (i.e., risks in centralized, TradFi systems). In other words, no trust of and reliance on any other person or entity is required for the system to function and the transaction to be carried out.

Reduced counterparty risk. Users are responsible for administering and managing their own assets. This not only allows users enhanced control, but interacting solely with software – rather than engaging in financial transactions through an intermediary – reduces counterparty risk in these transactions. Put simply, eliminating intermediaries and relying only on autonomous code reduces the risk of users having to rely on others for their transactions, whether for execution, for repayment of loans or the like for any other purpose.

Increased resilience. On a systemic level, smart contracts bring increased resilience to financial transactions by eliminating many points of failure – where financial institutions have been compromised from hacks and other types of exploits – and decentralizing the locus of transaction data and records, which, in the traditional world, are subject to hacks like those of Equifax,[47] the Consumer Financial Protection Bureau,[48] and SWIFT.[49]

3. *Bridges and zk Technology*

Bridges and zk technology also offer additional benefits to the blockchain ecosystem, primarily by enhancing its technological capabilities and fueling technological innovation.

Scaling and security. Bridges allow for blockchains to communicate and share data and assets with one another, spreading out transactions among blockchains versus having concentrated transactions in specific, discrete blockchains. ZKPs also improve scalability of L2s. ZKPs encrypt transactions – producing transaction hashes – in generating proofs, which are then used for validating. This reduces the computational load of processing transactions and allows L2s to scale, while decreasing transaction costs and increasing transaction speeds. Through encryption, ZKPs also safeguard private information of users by making it more difficult – although not impossible – to access. This affords users an added layer of privacy and protection, which also makes the network more secure as compared to its fully transparent L1 counterparts.

Innovation. Each blockchain network has its own ecosystem of developers, applications, and users. Due to the interoperability that bridges afford to blockchains, these individuals are able to

[46] *See e.g.*, https://cryptoforinnovation.org/key-elements-of-an-effective-defi-framework/
[47] *See e.g.*, https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach
[48] *See e.g.*, https://www.wsj.com/articles/in-major-incident-cfpb-says-staffer-sent-250-000-consumers-data-to-personal-account-fdc0a540
[49] *See e.g.*, https://medium.com/@kvantorcom/top-5-biggest-swift-hacks-52fca78145c

get exposure to and interact with *other* blockchain networks, fostering mutual growth among the different networks and promoting innovation (i.e., with more users comes more development and more innovation, which attracts additional users). ZKPs are also an emerging field in the blockchain industry that is fueling specific innovation in developing zk-based technology that can be used for a number of use cases, both financial (e.g., credit checks) and non-financial (e.g., digital identity).

IV. As Implemented, the Rule is Administratively Impracticable.

A. Given That Direct and Indirect Transactions Are Captured, It Is Impossible To Know Whether They are "Within or Involving a Jurisdiction Outside the United States."

We understand the proposed rule as concerning only mixers and mixing activity that occurs or is located *outside* the United States, in whole or in part. Indeed, this limitation would be necessary given the authority granted in 31 U.S.C. § 5318A(a)(1) ("1 or more classes of transactions within, or involving, a jurisdiction outside of the United States"), which explicitly speaks to "International Counter-Money Laundering Requirements." The factual predicate behind the Proposed Rule suggests the same limitation,[50] as implied in FinCEN's questions in its Request for Comments.[51] There is a distinct problem with this limitation.

For purely decentralized, non-custodial mixers, it will be impossible to determine whether any transaction relating to those mixers is "within or involving a jurisdiction outside the United States." These mixers – as well as DeFi, bridges and zk-powered L2s – are accessed through users' self-hosted wallets, which are pseudonymous and do not provide what is typically thought of as "personally identifiable information" – *e.g.*, name, email, address or even an IP address – that would otherwise link a user's wallet to a particular location. This is even more acute due to the fact that the Proposed Rule would impose enhanced recordkeeping and reporting requirements for *any* transaction that involves CVC mixing, meaning that there may be any number of pseudonymous transactions in the chain of the transaction that ultimately "makes its way" to a "covered financial institution." In other words, even if a covered financial institution collected and maintains jurisdictional information about the user seeking to engage in a transaction with the covered financial institution, if *any* transaction in the chain leading to the Final Transaction included or related to CVC mixing, it is still impossible to know the jurisdictions relating to those transactions in the chain and thus, impossible to know whether there is a non-US nexus to the Final Transaction.

[50] *See, e.g.*, NPRM at 72704 (assessment "that *foreign* CVC mixing transactions are used to facilitate or promote money laundering in or through jurisdictions outside the United States").
[51] *See, e.g.*, NPRM at 72711, Part VII.A., questions 4-7.

This inherent unknowability likely would result in one of three approaches – as discussed previously – by a covered financial institution: (1) apply the Proposed Rule to *all* transactions involving CVC Mixing (per the Proposed Mixing Definition); (2) apply the Proposed Rule to *none* of the transactions involving CVC Mixing; or (3) refuse to process any transactions otherwise "involv[ing]" CVC Mixing. In the event a covered financial institution continues to allow and/or process transactions "involv[ing]" CVC Mixing, the covered financial institution will be applying such requirements to nearly *all* blockchain transactions. For these reasons, the Proposed Rule is administratively impracticable as covered financial institutions will be required to engage in enhanced recordkeeping and reporting on almost *all* transactions if the Proposed Rule, with the Proposed Mixing Definition, is implemented as set forth in the NPRM.[52]

B. The Rule Requires Covered Financial Institutions to Undertake Duplicative Processes.

The Proposed Rule should also account for – and work in tandem with – the government's already-existing regulatory activities and authorities as they pertain to mixers and "mixing activity" including, but not limited to:

- Civil and criminal enforcement actions against mixers under the Bank Secrecy Act for failing to register as an MSB and for failing to maintain an appropriate AML compliance program;
- Civil and criminal actions against individuals and entities for committing substantive money laundering offenses, including those in connection with mixers and mixing activity;
- Civil and criminal actions against mixers for facilitating substantive money laundering offenses;
- Sanctions enforcement against mixers;
- Suspicious activity reporting by BSA-regulated entities (and voluntary SAR filings by non-regulated entities);
- Regulatory guidance by financial regulators and criminal law enforcement.

As currently constructed, the Proposed Rule will yield little, if any, benefit to law enforcement and other efforts to mitigate illicit finance. In fact, the new reports may dilute the existing pool of

[52] Separately as phrased, the Proposed Rule might appear or be interpreted to encompass transactions that are "within the United States" as well as those "involving a jurisdiction outside the United States." To address this potential ambiguity, at the very least the Proposed Rule should be modified to parallel the statutory language or otherwise expressly ensure that mixing activity with the United States is not within the scope of the rule.

actionable BSA reporting data with reports of questionable utility. This is because existing rules *already* require the reporting of suspicious activity in connection with convertible virtual currencies. Notably, "under the proposed rule, covered financial institutions would continue to have an obligation to file a SAR when warranted, regardless of whether the covered financial institutions also filed a report required under the proposed rule."[53] Similarly, the recordkeeping provisions are also in addition to, rather than in lieu of, the existing recordkeeping requirements.[54]

Thus, the resulting information that would be reported under the proposed rule falls under two categories: (1) information regarding *non*-suspicious transactions (or attempted transactions or patterns of transactions) which now must be reported; and (2) information regarding transactions (including attempted transactions or patterns or transactions) which are *already* reported under the SAR-reporting regime.[55] While the NPRM makes the assessment that there might be systematic underreporting of suspicious activity in connection with mixing activity, nothing suggests that the Proposed Rule would result in different reporting.

The converse is not true: under the Proposed Rule, there is a high likelihood that suspicious transactions are reported twice, demanding double the amount of compliance resources. Further, covered financial institutions' compliance departments will now also be required to report on transactions that they deem *not* suspicious.[56] As such, the Proposed Rule – if enacted – likely would operate to divert compliance resources away from specific investigations into actually suspicious activity in order to generate reports on a broad swath of transactional activity, licit and otherwise. As a corollary, the new information generated will demand double the amount of reviewing resources from law enforcement, intelligence community, and regulatory agencies that depend on these reports.

C. The Proposed Rule Is In Tension with other BSA/AML Requirements and The Equities.

[53] NPRM at 72711
[54] NPRM at 72722 n.181.
[55] There is arguably a third category of information that would be captured under the Proposed Rule, if enacted: suspicious transactions (or attempted transactions) which would otherwise be unreported because they fall beneath the transactional thresholds of the SAR reporting rules. *See, e.g.*, 31 CFR 1020.320(a)(2) (bank SAR rule imposing a $5,000 threshold); 31 CFR 1022.320(a)(2) (MSB rule imposing a $2,000 for reports by most types of MSBs). However, most of these smaller transactions, if suspicious, would nonetheless otherwise be captured under the existing rules as they would most likely be deemed as a part of "patterns" of suspicious transactions or one where the total amount "involves or aggregates" to the threshold limit, which would place it under the existing reportable rule.
[56] For this reason, FinCEN's position that "[i]n light of the existing compliance practices of covered financial institutions, FinCEN expects that complying with this proposed rule should not add a significant additional burden" (NPRM at 72710) is mistaken.

The increased requirements imposed by the new Proposed Rule will not only place further demands on compliance resources because of the duplication with existing BSA rules; to some extent, the new requirements may cause tension and friction with the existing BSA/AML regime.

The Proposed Rule may be more demanding and more onerous than those of SAR filing obligations.

First, the SAR rules typically require a report be filed within thirty days of the date of determining that the activity is suspicious.[57] But where the institution has not yet identified a subject, the institution has an additional thirty days to file – for a total of 60 days – a SAR. By contrast, the Proposed Rule requires filing of reports within 30 calendar days of initial detection of a covered transaction, regardless of whether a subject has been identified.

Second, for SARs, the "date of initial detection" is not when the transaction occurs or is highlighted for review, but typically when the financial institution reaches the conclusion in which it knows, or has reason to suspect, that the activity or transactions are suspicious.[58] The reports under the Proposed Rule contain no such limiter, but only as within 30 calendar days of when the covered transaction is initially detected, regardless of whether it is considered suspicious.

Third, unlike the SAR rules, the Proposed Rule lists a number of items and data fields not typically provided in a SAR.[59]

Finally, the existing SAR rules require the financial institutions to maintain their required BSA records for at least five years. The Proposed Rule, however, goes a step further, requiring – though not explaining – that a covered financial institution must also "document its compliance with the requirements of this section."

The Proposed Rule omits an important protection that the SAR rules guarantee: an obligation of confidentiality on recipients. The unauthorized disclosure of SARs "compromises the essential role SARs play in protecting our financial system and in preventing and detecting financial

[57] 31 CFR 1022.320(b)(3), which governs most MSBs, provides that the financial institution must file "no later than 30 calendar days after the date of the initial detection by the money services business of facts that may constitute a basis for filing a SAR under this section." Other financial institutions are covered by substantially similar language. See 31 CFR 1020.320 (banks); 31 CFR 1021.320 (casinos and card clubs).

[58] See FinCEN, SAR Activity Review: Trends, Tips, & Issues, Issue 10 (2006), *available at:* https://www.fincen.gov/sites/default/files/sar_report/sar_tti_10.pdf.

[59] NPRM at 72722-23. Although the Proposed Rule purports to limit the reportable information to that which is "in the possession" of the financial institution, in practice the result will be much different. Covered Financial Institutions will certainly be required to investigate potentially-reportable transactions, if for no other reason than to "document [their] compliance. And the NPRM itself confirms this in describing what should be contained in the Narrative section of the report: "The proposed rule would require a description of activity observed by the covered financial institution, including a summary of investigative steps taken, provide additional context of the behavior, or other such information the covered financial institution believes would aid follow on investigations of the activity." NPRM at 72711.

crimes and terrorist financing."[60] The confidentiality rule provides an essential safeguard for both the underlying investigations, as well as for those required by the rules to report on activity.

Under the statutes and regulations, suspicious activity reports are protected from disclosure other than in very narrow circumstances.[61] Unauthorized disclosure of SARs constitute violations of federal law, and the government may impose civil and criminal penalties for these violations.[62] There are several reasons for this strict confidentiality: (1) investigations might be compromised by tipping off subjects and their co-conspirators; (2) financial institutions would be deterred from filing SARs if they knew that their SARs would be exposed; (3) individuals and companies named in the SAR would suffer reputational damage if SARs were public; and (4) to prevent reprisal for SAR filing and thereby to protect the safety and security of financial institutions and financial institution employees who file the reports. As FinCEN noted, "[t]he success of the SAR reporting system depends on the financial sector's confidence that these reports will be appropriately protected."[63]

The Proposed Rule offers no such protection, and no such confidence. There appears to be no statutory or regulatory provision for nondisclosure, or a means to limit those documents from production to outside parties, including in litigation. There is no penalty, and although SARs may also be filed for such activity, the reports contemplated by the Proposed Rule would not "reveal the existence or nonexistence of a SAR" and so it would not be shielded from disclosure.[64]

D. The Impracticability of Implementing the Rule Will Thwart Legitimate U.S. National Security Interests.

The overbreadth of the CVC Mixing Definition and the related impracticability of implementing the Proposed Rule likely will have unintended, adverse consequences for U.S. national and economic security. Specifically, and as discussed above, the Proposed Rule is so broad that covered financial institutions likely will refuse to process or otherwise engage in *any* transactions that it "knows, suspects, or has reason to suspect" involves CVC Mixing.

---

[60] FinCEN Advisory FIN-2012-A002, *SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions*, (March 2, 2012), *available at:* https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A002.pdf.

[61] See 31 U.S.C. 5318(g)(2); 31 C.F.R. 1020.320(e); 31 C.F.R. 1022.320(e); see also FinCEN Advisory FIN-2010-A014, *Maintaining the Confidentiality of Suspicious Activity Reports* (November 23, 2010), *available at:* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a014.

[62] 31 U.S.C. 5321 (civil penalties); 31 U.S.C. 5322 (criminal penalties, including up to five years of imprisonment per violation).

[63] FinCEN Advisory FIN-2010-A014, *supra* note 61.

[64] Financial institutions that file SARs are also protected from liability for such filings because of a statutory "safe harbor" protecting them from liability for such filings. *See* 31 U.S.C. 5318(g)(3); 31 C.F.R. 1020.320(f); 31 C.F.R. 1022.320(f). These rules shield institutions (and their employees). It is possible that these filings would qualify under the regulation that provides for a limitation on liability for other "disclosure[s] of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this section or or any other authority." See, e.g., 31 CFR 1022.320(e). However, the Proposed Rule itself is silent as to whether such protection would attach, and it is unclear whether these filings under the Section 311 authority would fall under this safe harbor.

In practice, this means that *no* U.S. covered financial institutions subject to the BSA would engage in transactions involving CVC Mixing. Although there may be some argument for curtailing CVC mixing transactions in such a significant way,[65] the Proposed Rule will only curtail these transactions for *U.S.* covered financial institutions or others that are subject to the U.S. AML/CFT regime. Non-U.S. VASPs, however, process or engage in a significant amount of blockchain transactions.[66] In other words, non-U.S. VASPs will continue to process transactions "involv[ing]" CVC mixers, but these transactions will *not* be subject to any recordkeeping or reporting requirements – enhanced or otherwise. Indeed, according to statistics from both Treasury and FATF, non-U.S. VASPs have the highest level of *noncompliance* as it relates to AML/CFT monitoring and deterrence.[67]

Moving all CVC mixing transactions to off-shore, non-U.S. VASPs would remove any visibility into CVC mixing activity for FinCEN, and for U.S. law enforcement and the intelligence community. This would thwart the purpose of the BSA's recordkeeping and reporting requirements – *i.e.*, to allow U.S. law enforcement to detect, investigate and prosecute potential illicit actors.

That the Proposed Rule would have these unintended consequences and ultimately hamper the purpose of the Proposed Rule – "to defend the U.S. financial system from money laundering and terrorist financing"[68] and to allow U.S. law enforcement "to better understand the illicit finance risk posed by CVC mixing and investigate those who seek to use CVC mixing for illicit ends"[69] – is a distinct and independent reason that the Proposed Rule should not be implemented as currently formulated.

V. An Alternative Path Forward

As outlined above, the Proposed Rule involves a number of problems ranging from overbreadth to impracticability to inconsistency with the underlying Section 311 statute to friction with the overall BSA/AML regime. We share FinCEN's concern that crypto and the blockchain ecosystem should not be a haven for money launderers, terror financiers, fraudsters, sanctions

[65] *Ibid.* (" . . . it may be reasonable to expect that the number of CVC mixers that can concurrently achieve and maintain a sustainable scale to continue operations is unlikely to grow.").
[66] FATF alone looked into 98 jurisdictions. *See* FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" 2 (June 2023), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf.
[67] *See* U.S. Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," 29 (April 2023), available at: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf ("The 2022 NRAs identified that the most significant illicit financing risk associated with virtual assets stemmed from VASPs operating abroad with substantially deficient AML/CFT programs, particularly in jurisdictions where AML/CFT standards for virtual assets are nonexistent or not effectively implemented."); *see also* FATF, *supra* note 76 ("However, it is a serious concern that 75% of jurisdictions assessed against the revised standards are only partially or non-compliant with FATF's requirements.").
[68] NPRM at 72701.
[69] NPRM at 72706.

evaders, and others seeking to use the technology for illicit purposes. This is not simply because of corporate citizenship; it is also because the survival of this industry depends on legitimacy, trust, and the fact that users will never participate in a system which is also a home to those who finance North Korea's weapons programs, fraudsters engaged in pig butchering, Russian state actors seeking to avoid sanctions, or others who intend to use the blockchain for illegal ends.

And this is why any rules and regulations must address the threat directly. They should do so in ways that neither push the technology offshore (and beyond the reach and visibility of U.S. law enforcement), nor undermine the overall BSA/AML regime by imposing an inefficient, resource-draining, and broad-brush stroke approaches that don't fully account for legitimate uses of the affected technologies.

As discussed above, any proposed regulatory action should take into account the existing BSA/AML regime. Treasury, together with law enforcement and the intelligence community, can provide guidance to industry about specific technologies, practices, and transaction flows involving efforts to obscure illicit proceeds. These can be through mechanisms such as 314a information sharing, 314b programs, industry outreach, and public-private partnerships.

There is ample precedent for this approach. For instance, for the casino and card club industry, FinCEN has promulgated a set of "red flags" for those operators to identify, detect, report, and prevent certain illegal activity.[70] In fact, FinCEN has already done this regarding various topics, including identifying typologies and red flags regarding Russian illicit finance, Hamas, human trafficking, fraud schemes, public corruption, and a host of other illicit finance topics. Other agencies and intra-agency organizations (such as the FFIEC), as well as foreign inter-governmental organizations (such as the Financial Action Task Force) have similarly provided guidance to the private sector to encourage and inform their suspicious activity reporting and other anti-money laundering prevention efforts.

And FinCEN has already promulgated such reports regarding virtual currencies.[71] Notably, in providing this guidance regarding SAR reporting concerning these red flags:

> "Because some red flags associated with abuse of CVC may reflect legitimate financial activities, financial institutions should evaluate indicators of potential CVC misuse in combination with other red flags and the expected transaction activity before determining that a particular transaction is suspicious. Due to the

[70] FinCEN Advisory FIN-2008-G007, *Recognizing Suspicious Activity - Red Flags for Casinos and Card Clubs* (August 1, 2008), *available at:* https://www.fincen.gov/resources/statutes-regulations/guidance/recognizing-suspicious-activity-red-flags-casinos-and-card.
[71] *See, e.g.,* FinCEN Advisory FIN-2019-A003, *Advisory on Illicit Activity Regarding Convertible Virtual Currency* (May 9, 2019), *available at:* https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

> technical nature of blockchain analysis and other frameworks of analyzing CVC activity, FinCEN encourages communication within financial institutions among AML, fraud and information technology departments, as appropriate. FinCEN also encourages communication among financial institutions under the auspices of Section 314(b) of the USA PATRIOT Act in determining transactions' potential suspiciousness related to terrorist financing or money laundering activities, and in filing SARs, as appropriate."[72]

FinCEN's existing SAR-reporting rules provide the appropriate vehicle for reporting actual and potential illicit finance threats by mixers and mixing technology. This alternative carries a number of advantages. First, rather than a wholesale sweep of an entire industry and its related ecosystem, a guidance-plus-SAR-reporting approach allows financial institutions and law enforcement alike to focus their resources on the actual threats – "illicit activities using CVC mixing in furtherance of their unlawful objectives" and "the use of CVC mixing in connection with money laundering and other financial crimes." Second, it avoids the situation where, as under the Proposed Rule, financial institutions would be required to (1) report on *non-suspicious* activities;[73] (2) report multiple times on the same transaction, and using multiple forms and with different standards and timeframes; (3) creating a system without the important protections of confidentiality (and possibly without safe harbor protection) by having a non-SAR filing.

In short, FinCEN may be appropriately concerned about illicit money flows traveling through mixers and mixing activity generally. Financial institutions should be equally concerned. But the remedy is important. The best approach to detect, report, and prevent such illicit activity is not with an all-inclusive recordkeeping and reporting regime which does not depend on whether a transaction is "suspicious" and takes no account of the already-existing BSA/AML framework. Nor is it one that acknowledges that some mixing activity is for legitimate purposes, but which does not tailor its requirements to navigate those concerns. Nor is it one that imposes serious duplicative obligations and without the necessary confidentiality and safe harbor safeguards. Rather, we respectfully submit that the Treasury can best address its legitimate concerns by using its existing suspicious activity reporting obligations – coupled with industry outreach and law enforcement information sharing – to obtain the information and assessment it requires.

* * *

[72] *Ibid.* at 11.
[73] As a corollary to this, it avoids the untenable situation under the Proposed Rule where the "implied burden would shift from determining when a CVC transaction is reportable to determining when it is not reportable." NPRM at 72713.

We appreciate the opportunity to provide comments with respect to rule-making that could potentially affect how all parts of the blockchain ecosystem, most notably zk-based technology, bridges, and DeFi protocols, are used and may develop in the future.

Polygon Labs and DELV are available to meet and discuss the points and recommendations in this response further and respond to any questions.

Sincerely,

Rebecca Rettig
Chief Legal & Policy Officer

Katja Gilman
Senior Public Policy Lead
Polygon Labs

Gregory C.J. Lisa
Chief Legal Officer
DELV