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

FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB547

January 4, 2021

To Whom it May Concern:

ConsenSys Software Inc., a U.S. headquartered Delaware corporation, is among the software engineering leaders of the blockchain space. Our full-stack Ethereum products help developers build next-generation networks and enable enterprises to launch more powerful infrastructure. To date, our products have on-boarded over one million users globally to Ethereum-based decentralized technologies, including dozens of the world's most reputable institutions. We comment in our capacity as a company impacted by your proposed rules, but also as a steward of what we view as Web 3.0[1], the inevitable evolution of our existing infrastructure to an infrastructure that reduces trust and reliance on third parties, while increasing transaction speed, decreasing fees, opening access to financial services, and restoring both privacy and security to users. We do not believe the evolution to Web 3.0 requires impairment of our ability to prevent nefarious actors. Web 3.0 technologies and our correlated privacy goals do not seek to permanently obfuscate - rather they focus on enhanced transparency and traceability with privacy as a feature - not a permanent state - allowing law enforcement to fulfill their remit while simultaneously restoring privacy norms that eroded through the evolution of Web 2.0. We are confident that if the Treasury works together with industry, we can ensure the same or better outcomes while still achieving the promises of better privacy, security, access, and savings - and in so-doing, keeping the United States of America the financial center of the globe.

---

[1] https://www2.deloitte.com/us/en/insights/topics/digital-transformation/web-3-0-technologies-in-business.html

Our comment is structured in two sections, the first with points generally applicable to the entire Notice of Proposed Rulemaking (the "NPRM"), and the second, focused more directly on the proposed recordkeeping requirements. We thank you for your consideration of these comments, and as always, we are happy to serve as a resource to you both formally and informally, as we do for regulatory bodies globally on a routine basis.

1. Comments Generally Applicable to the NPRM

(a) Exigency and Due Process - Errors Compounding the Risks Posed by Subsequent Commentary

As explained in the following section, what FinCEN may describe as Convertible Virtual Currency ("CVC") or Legal Tender Digital Assets ("LTDA") is likely to be the entire universe of commodities, currencies, and all manner of property. FinCEN has determined that it is appropriate to provide a 15 day period for public comments, comments which FinCEN, under ordinary circumstances, would be required to consider, but here, as FinCEN indicates, such requirements are inapplicable. In citing national security imperatives and the exigency of the risk warranting a 15 day comment period—with most days occurring on Federal and business holidays—FinCEN seeks to publish rules that go far beyond the scope of "illicit finance." These rules will impact not only finance and financial instruments, but software development, art, real estate, and innumerable activities and industries that may touch the broad bucket FinCEN describes as a CVC or LTDA.

The first citation FinCEN relies on to support exigent circumstances is a case filed on June 1, 2017, *1,313 days* between the filing of that case and the date this comment will be filed. The United States has long had a reputation, unlike its contemporaries in Europe and Asia, for being hostile to virtual currency and broader blockchain technology, and this NPRM and condensed and/or ignored comment period will only serve to further that narrative. We respect FinCEN's remit, but would urge FinCEN to consider expanding the public comment period, as the engagement FinCEN cites is simply insufficient to understand the broad impact of these rules.

As a publisher of the leading self-hosted wallet for Ethereum, we routinely work with law enforcement agencies around the globe in such jurisdictions as the United Kingdom, Japan, Singapore, Ireland, Germany, and many others, who serve lawful process when seeking to investigate crimes. We note that the ratio of requests served by United States law enforcement is a mere fraction of what we receive from international authorities, and in a proper comment period we would work to explain how existing forensic technology and legal processes *may* serve to add additional comfort, perhaps mitigating the need for some of the expansiveness found in the NPRM.

Chiefly, we are concerned that the logic being employed to justify the truncated due process sets the stage for subsequent rulemakings—raising the potential to perpetually deprive an entire industry of due process merely because a rulemaking involves a "CVC" or "LTDA." Respectfully, this significantly risks the United States losing its preeminent role as the world's financial leader and stunting the cornerstones of American economic dominance: innovation and technology.

(b) Generalization of the term "CVC" or "LTDA"

Blockchain technology, most specifically Ethereum, enables the frictionless creation of what we regard as a digital asset. The term digital asset is a category, simply defined as any asset that can be represented by a digital identity, colloquially known in many circles as a "token." The primordial blockchain application gave us the digital asset Bitcoin, the application of the bitcoin blockchain. Ethereum enabled tokens to take many different forms beyond that of Bitcoin, which is most commonly viewed as a currency or store of value. To date, Ethereum has inspired the creation of digital assets that may represent:

- Digital Asset Securities
- Digital Art
- Digital Collectibles
- Digital Currency
- Digital Commodities
- Digital Playing Cards and Video Game Items
- Digital Governance Rights
- Digital Representations of Identity and Reputation

- Digital Representations of Real Estate
- Digital Representations of other Intellectual and other Property Rights

Classification and regulation of these assets presents many challenges for regulators around the globe, and we've appreciated the nuanced approach taken by regulators in the United States, most specifically the Securities and Exchange Commission and the Commodities and Futures Trading Commission, who have been exemplary in recognizing that not all digital assets fit into the same box[2]. It is this thoughtful approach, one employed nearly globally, that has allowed digital assets to emerge, thrive, and begin to deliver on the core promises of this technology which we outlined in our introduction.

The NPRM unfortunately seeks to generalize an entire industry of digital assets into two buckets: Convertible Virtual Currency or Legal Tender Digital Assets. Both terms purport to encompass the entire universe of digital assets, creating an unfortunate outcome where FinCEN seeks to impose rules relating to currencies on not only digital currencies, but also on digital art, digital collectibles, digital software licenses, and a whole host of both fungible and non-fungible digital goods, both existing and yet to be created, that will now fall within the scope of the proposed rules. In doing so, FinCEN will add obligations and burdens to entire industries and asset classes merely because they are represented as a digital asset. We deeply respect and agree with the aims of FinCEN, mainly preventing financial crimes and terrorist activity, but the proposed NPRM and its definitions mirror a blunt instrument, not a targeted tool to achieve its purported aims.

(c) Unintended Consequences - The Threat Posed to Law-Abiding Americans

As we are all aware, and as your NPRM indicates, cybercrimes continue to escalate. The product of the reporting and recordkeeping requirement will be the creation of lucrative stores of data in both private enterprise and at the Treasury/related agencies. While growing in popularity, blockchain technology is still nascent and measures by which individuals safeguard their digital assets are far from impenetrable, particularly in light of the absence of meaningful regulation of third parties, such as the leading Telco companies, which have allowed several years of unabated SIM-swapping[3] attacks on honest Americans, including many of our

[2] https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf
[3] https://www.wired.com/story/sim-swap-attack-defend-phone/

employees, leading to financial theft in the hundreds of millions, if not billions of dollars. ConsenSys has worked actively with leading enforcement agencies, like the Manhattan District Attorney's Office, who nobly pursue these criminals, but their efforts alone are not enough. As a company, we've pleaded with both Federal and State Attorneys General—the only groups with enough authority to actually penetrate through to a Telco—to take meaningful action and force these Telco companies to take reasonable measures to stop these crimes, pleas that have fallen on deaf ears.

When there is inevitably a data breach, either at a private MSB[4] or the Federal[5] government itself, those who wish to commit SIM-swapping, phishing, and more violent crimes to extract virtual currency from hard-working and law-abiding citizens will receive the equivalent of an invitation to pillage those whose data is exposed. As a company, we are working on privacy preserving technologies, not as a means to circumvent regulation, but as a means to move us to a world where we can verify lawful behavior in a manner that does not lead to these events, which we hope you understand are in fact inevitable given the type of data and scope of the requirements put forth in the NPRM. If FinCEN is to move ahead with the proposed rules without limiting the scope and preservation requirements found therein, we urge FinCEN to work with the appropriate Federal and State agencies to see that there are reasonable measures being taken to help prevent this avoidable harm to Americans—harm that will be a direct result of this rule. As indicated earlier, losses due to these crimes already likely tip over into the billions, and we are gravely concerned the proposed rules will be an exponent to that figure, leading to legitimate questions about whether this rule will be a net benefit or harm to the American public.

2. Comments Applicable to the Proposed Recordkeeping Requirement

Notwithstanding the security, overly broad classifications, and due process concerns raised above, we are inclined to agree with FinCEN that the *reporting* requirements are generally reasonable with respect to digital currency in light of obligations imposed on MSBs dealing in traditional currency. One cannot send a $10,000 wire today without there already being informational requirements satisfied on both ends of the transaction. We do however

---

[4] https://selfkey.org/list-of-cryptocurrency-exchange-hacks/

[5] https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/

object to the proposed recordkeeping requirement, one that we were taken aback by as we read the full notice. The notice asserts "[t]his proposed rule would add a new recordkeeping requirement at 31 CFR 1010.410(g) requiring banks and MSBs to keep records and verify the identity of *their* hosted wallet customers, when *those customers* engage in transactions with unhosted or otherwise covered wallets with a value of more than $3,000."

The proposed rule differs materially from its explanation in the notice summary. In fact, the proposed rule requires the bank or MSB to obtain and preserve "(vii) The name and physical address of each *counterparty* to the transaction of the financial institution's customer, as well as other *counterparty* information the Secretary may prescribe as mandatory on the reporting form for transactions subject to reporting pursuant to §1010.316(b)." This counterparty information requirement is a substantial departure from the way the recordkeeping rule is described in the notice, merely indicating a bank or MSB would be required to keep records of *their* customers transactions.

We fear the result of this rule will be several prong:

A. It will add additional compliance costs to banks and MSBs dealing in CVC or LTDA that are not borne by those not dealing in these assets, merely by the nature in which these transactions routinely take place as described above. The end result could be fewer institutions providing these services, limiting access, competition, and innovation in the United States;
B. The rule will enable banks and MSBs to collect information that will allow them to further discriminate against certain types of lawful transactions that banks or MSBs are encouraged to prohibit on a political or moral, but not legal, basis, such as what we've seen under the Operation Chokepoint[6] initiative. When paired with the unintended consequence of limiting service providers due to compliance burdens, we believe the Treasury should complete a policy analysis to determine whether or not these requirements may only further limit access to financial services for law-abiding citizens of this country; and
C. The rule will ultimately jeopardize the security of Americans who would otherwise transact between regulated and insured institutions, by giving many an impossible dilemma: sacrifice their and their counterparty's privacy, particularly in light of the

[6] https://www.americanbanker.com/opinion/theres-no-downplaying-the-impact-of-operation-choke-point

security and policy risks described above, or force them to transact through other, potentially less secure - and less traceable means.

As we do not run a bank or MSB, we cannot comment on the impact analysis figures provided by Treasury estimating the burden of these rules, but we do know it is likely impossible to properly analyze the accuracy of those figures in 15 days, and even further, as consumers ourselves, we know we will ultimately be “passed the buck” on these additional costs. We therefore request the Treasury consider amending the proposed recordkeeping requirement by eliminating section (vii) regarding counterparty information, or short of that, consider raising the transaction threshold to ensure records only need to be preserved - then deleted - for a time period that is directly proportional to any benefit the proposed rule seeks to achieve.

3. Conclusion

We respect and encourage the work done by Treasury and prominent global regulatory agencies to help provide sustainable regulatory frameworks that achieve their stated objectives while avoiding unintended consequences—consequences in this case which may amount to unexpected harm to Americans and impairment of innovation in the United States. We encourage FinCEN and the Treasury to consider these comments and to work further with industry to promote regulations that achieve their stated aims, protect Americans, and do so in a manner that keeps the United States competitive.

Respectfully Submitted on Behalf of ConsenSys Software Inc.,

Matt Corva
General Counsel