Comments on the Financial Crimes Enforcement Network's Notice of Proposed Rulemaking on "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets"

January 2021

The Blockchain Association
1701 Rhode Island Avenue N.W.
Washington, D.C. 20036

January 4, 2021

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

Re: FinCEN Docket No. FINCEN-2020-0020; RIN 1506-AB47

To whom it may concern:

The Blockchain Association submits these truncated comments in response to the Notice of Proposed Rulemaking (the "NPRM") titled "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Fed. Reg. 83,840 (Dec. 23, 2020) within the extremely truncated comment period set forth in the NPRM. The Blockchain Association is a not-for-profit organization dedicated to improving public policy in ways that will help blockchain networks and their users develop and prosper in the United States. Its diverse membership reflects the complexity of this dynamic market and includes projects building blockchain networks, trading platforms that allow users to exchange cryptocurrencies, and early stage investors that support the entire ecosystem. The Blockchain Association comprises industry leaders who are committed to responsibly building, funding, and supporting blockchain networks fueled by cryptocurrencies. It endeavors to educate policymakers, courts, and the public about how blockchain technology works and how regulatory clarity can bring about a more secure, competitive, and innovative digital marketplace. Given its diverse membership, the Blockchain Association would be well positioned to provide FinCEN and the Department of the Treasury with the valuable perspectives of those who facilitate and engage in transactions involving convertible virtual currency or digital assets with legal tender status held in self-hosted wallets if only the NPRM allowed for sufficient time for consultation and data gathering. Having been given only a scant comment interval over the holidays, the Association has done its best to assemble comments that reflect the incomplete and cursory information that could be assembled under the circumstances. While the Association would have even more to say if it were afforded a reasonable comment period, the Association firmly believes that the NPRM suffers deep procedural and substantive flaws.

1) The NPRM Is Procedurally Defective.

The Association and other members of the cryptocurrency community are eager to work with FinCEN and the Department of the Treasury to help craft policies that accomplish the government's important regulatory objectives without unnecessarily curbing innovation or treading on individuals' property and privacy rights. But assembling diverse perspectives and achieving regulatory balance takes time. The rushed timeframe reflected in the NPRM has severely frustrated the Association's ability to provide vital input. The Blockchain Association urges the Department of the Treasury to extend the comment period for the NPRM to at least 60 days, so that all interested parties—including the Association, FinCEN and the Department—can give these important and complex issues the serious attention that they deserve.

The 72-page NPRM was announced late in the day on Friday, December 18, 2020. Although the NPRM promised a mere 15 days for comments, the comment period did not actually open until December 23, 2020, leaving just 12 days for interested parties to submit comments. That 12-day window spanned a major holiday period that included Christmas Eve, Christmas (a federal holiday), New Year's Eve, New Year's Day (another federal holiday), and four weekend days. Some foreign countries in which stakeholders operate observe additional national holidays. That left interested members of the public with, at best, a grand total of seven "working days" to comment on an NPRM that seeks feedback on more than three times as many topics. That amount of time is plainly insufficient to submit meaningful, substantive comments. For example, at least six members of the Blockchain Association would be required to comply with the proposed rule, but only one of the six was able to provide preliminary data on the burdens the proposed rule would impose within the extremely abbreviated comment period. That unduly truncated comment period runs roughshod over both fundamental tenets of good governance and the requirements of the Administrative Procedure Act ("APA").

Perhaps anticipating objections to the unreasonable comment period, the NPRM suggests that even this minimal nod to notice and comment is a matter of administrative grace, because FinCEN need not engage in any notice and comment at all. But the stated excuses for evading bedrock APA requirements are unavailing. The NPRM first posits that the rule implicates a "foreign affairs function," and so is exempt from notice and comment rulemaking entirely. See 85 Fed. Reg. at 83,852; 5 U.S.C. §553(a)(1). But that a rule "implicates foreign affairs … is not enough to satisfy the foreign affairs function exception." *Capital Area Immigrants' Rights Coalition v. Trump*, 471 F. Supp. 3d 25, 56 (D.D.C. 2020). Instead, that narrow exception is satisfied only when a rule "clearly and directly involve[s] activities or actions characteristic to the conduct of international relations." *Id.* at 53; *see also, e.g.*, *City of New York v. Permanent Mission of India to United Nations*, 618 F.3d 172, 202 (2d Cir. 2010). A rule that regulates wholly private financial transactions that may (or may not) involve foreign actors undoubtedly does not satisfy that demanding standard. Indeed, if the mere fact that financial transactions may involve foreign actors were enough to take a rule outside the APA, then Congress would not have needed to amend the Bank Secrecy Act ("BSA") to craft special procedures (not applicable here) that allow certain types of regulations of transactions with foreign entities to take temporary effect while notice and comment is ongoing. *See* 31 U.S.C. §5318A. As that limited and inapplicable exception reflects, it has long been settled law that the foreign affairs "exception cannot apply to functions merely because they have impact beyond the borders of the United States." *Mast Industries, Inc. v. Regan*, 596 F. Supp. 1567, 1581 (Ct. Int'l Trade 1984).

Nor would the APA's "good cause" exception apply here. *See* 5 U.S.C. §553(b)(3)(B). The good cause exception is "meticulous and demanding." *Sorenson Commc'ns Inc. v. FCC*, 755 F.3d 702, 706 (D.C. Cir. 2014). It is "narrowly construed and only reluctantly countenanced," with the agency bearing the burden of persuasion, and doing so without the benefit of any deference. *NRDC v. NHTSA*, 894 F.3d 95, 113-14 (2d Cir. 2018). The NPRM posits that "[u]ndue delay in implementing this rule would encourage movement of unreported or unrecorded assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets." 85 Fed. Reg. at 83,852. But the key phrase in that sentence is "undue delay." In circumstances where some notice and comment period is feasible, as it is here, the APA determines that a delay for a period to allow for meaningful notice and comment is not just due, but legally required. By allowing even an extremely truncated comment period before the proposed rule takes effect, FinCEN has acknowledged this is *not* the rare situation where the rule must be imposed immediately to prevent circumvention. Where some comment period is viable, the APA demands a meaningful comment period, not 15 days over the holidays. And while the NPRM notes that "the prevention of substantial financial fraud" may constitute good cause, 85

Fed. Reg. at 83,853 (citing *Disabled in Action of Metro. New York, Inc. v. Brezenoff*, 506 F. Supp. 244, 248 (S.D.N.Y. 1980)), FinCEN has identified nothing even remotely comparable to the ongoing, multimillion-dollar fraud on a federal program that justified immediate agency action in *Brezenoff*.

For all of those reasons, the Blockchain Association strongly urges FinCEN to extend the comment period to at least the standard 60 days. The Association's counsel sent a letter to Secretary of the Treasury Steven Mnuchin requesting an extension of the truncated notice and comment period. That letter is included as an addendum to this comment.

2) The Proposed Rule Would Constitute An Unprecedented and Untested Expansion of the BSA to Include Collection Of Counterparty Information.

The proposed rule would represent a novel and dramatic expansion of the scope of the BSA and FinCEN's authority thereunder. The NPRM characterizes the proposed requirements as merely "a targeted expansion of BSA reporting and recordkeeping obligations." 85 Fed. Reg. at 83,841. But in reality, the proposed rule seeks to do much more than that. It would impose novel requirements on MSBs to ascertain, record, and report to the government information about individuals with which they have no relationship. It is one thing to know your customer, and quite another to know your customer's customer or counterparty. That is not just a difference in degree, but a difference of kind, as demanding information about a customer's customer effectively converts an MSB from a regulated party to a *de facto* regulator of its customer's downstream transactions.

The proposed rule would require MSBs that facilitate transactions in convertible virtual currencies to: (1) "file a report with FinCEN containing certain information related to a customer's CVC [convertible virtual currency] or LTDA [legal tender digital assets] transaction and counterparty (including name and physical address), and to verify the identity of their customer, if a counterparty to the transaction is using an unhosted or otherwise covered wallet and the transaction is greater than $10,000 (or the transaction is one of multiple CVC transactions involving such counterparty wallets and the customer flowing through the bank or MSB within a 24-hour period that aggregate to value in or value out of greater than ($10,000)"; and (2) "keep records of a customer's CVC or LTDA transaction and counterparty, including verifying the identity of their customer, if a counterparty is using an unhosted or otherwise covered wallet and the transaction is greater than $3,000." *Id.* at 83,843. In other words, the proposed rule would require MSBs to proactively collect, record, and report information about their customers' *counterparties*—individuals with whom those financial institutions may have no relationship whatsoever.

That is a radical expansion of MSBs' obligations under the BSA. While the BSA authorizes the Secretary to require an MSB to "file a report on the transaction at the time and in the way the Secretary prescribes," 31 U.S.C. §5313(a), that authority has never before been invoked to require MSBs to ascertain and report information about their customer's counterparties. No existing BSA-related reporting or recordkeeping requirements mandate the collection of information about the *counterparties* with which MSB customers transact. In fact, the word "counterparty" does not appear in any regulation issued by FinCEN, *see* 31 CFR Ch. X, §§1000-1099, or in the Federal Financial Institutions Examination Council's manual; *see* https://bsaaml.ffiec.gov/manual. MSBs do not regularly require their customers to provide counterparty information in order to receive financial services, so they do not have any counterparty information to "keep" or to "file" beyond what is available on transparent blockchains. Nor, based on the cursory information we have been able to assemble during the truncated comment period, does it appear that they even

have the means to acquire such information. Making matters worse, the NPRM does not even purport to identify all of the information it is proposing to require banks and MSBs to obtain and report. *See, e.g.*, 85 Fed. Reg. at 83,861 (proposing that requirements will *include* "[t]he 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*") (emphasis added).

The proposed rule would thus chart potentially dangerous new regulatory territory. The leap from knowing your customers to knowing your customer's counterparty is no small step, but would convert MSBs into *de facto* regulators. It is unclear that the relatively modest authorization to require MSBs to maintain records about their own customers implicitly includes this much greater authority to superintend the counterparties with whom a customer interacts. Nor is it obvious that, if such an authority existed, it would be limited to counterparties and not extend to the counterparties' counterparties, and so on. Nothing in the existing statutory and regulatory realm clearly sanctions requiring MSBs to undertake such an essentially regulatory task, and FinCEN should be loath to assign such a novel task in the absence of express statutory authority (and certainly not through a highly expedited rulemaking).

3) MSBs Would Be Unable To Comply With The Proposed Rule.

Precisely because there are no existing mechanisms for even obtaining the information the proposed rule would demand, the rule would likely operate as a *de facto* ban on certain transactions, at least while MSBs develop ways to comply with the proposed rule. Because a requirement to identify counterparties is completely novel to the BSA regime, regulated entities would have to develop wholly new procedures to acquire, maintain, and report the information that the proposed rule would require. Contrary to the NPRM's suggestion, there are no existing "risk-based procedures" "consistent with their AML/CFT programs" for financial institutions to "continue to follow" in order to comply with the proposed rule because none of those procedures applies to counterparties. *See* 85 Fed. Reg. at 83,849-50. Faced with wholly new regulatory obligations in an unprecedentedly short time frame, MSBs could either: (1) quickly develop new processes and hope they are acceptable to FinCEN (the technical challenges of which are explored below); or (2) cease facilitating transactions involving third parties to avoid triggering the requirements at all. The first option appears infeasible in the short run. Thus, as a practical matter, the rule would likely operate as a *de facto* ban on financial institutions transacting with self-hosted cryptocurrency wallets. That is doubly problematic. First, imposing a *de facto* ban while justifying only a regulatory reporting requirement is the essence of arbitrary and capricious decisionmaking. Second, it is far from clear that FinCEN would have the power to prohibit such transactions, which makes its apparent attempt to accomplish that end indirectly all the more legally suspect.

A threshold problem with the proposed rule is that associating cryptocurrency wallets' private keys with individual users is both impractical and of limited utility. As the Securities and Exchange Commission has explained, an individual or entity "may not be able to demonstrate that no other party has a copy of the private key and could transfer the digital asset[s] …." U.S. Securities and Exchange Commission, Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (July 8, 2019), *available at* https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities. In other words, the fact that one individual (or hypothetically "identified" counterparty) has access to a private key associated with a certain cryptocurrency address does not mean that the individual exercises *exclusive* control over the associated digital assets. Just as an MSB is unable to reasonably determine that a person in possession of a physical wallet has ongoing exclusive control and ownership of the cash stored in it, it is impossible to determine whether a cryptocurrency private key is under the

exclusive control and ownership of the person using that key. Accordingly, to the extent the proposed rule would require MSBs to identify who has *exclusive* control over the wallets with which their customers transact, then MSBs may reasonably conclude that the only path to compliance would be to avoid triggering the requirements at all by prohibiting transactions involving self-hosted wallets held by third parties or wallets hosted by certain foreign financial institutions. The NPRM never even acknowledges this serious problem, let alone attempts to address it.

Compounding that problem, the proposed rule fails to clearly define the types of transactions subject to additional recordkeeping and reporting requirements. The rule only addresses transactions between a hosted wallet and a self-hosted wallet controlled by a single counterparty, but that type of transaction accounts for a small and decreasing amount of total activity on public blockchains. Much of the innovation taking place in the blockchain industry is being driven by "decentralized finance," which refers to software protocols that allow users to engage in a broad range of economic activities without the need to rely on trusted third parties. Transactions can occur between a hosted wallet and a "smart contract," an autonomous, self-executing software protocol that has no legal name or physical address to record or report. The proposed rule does not even reflect the technical possibility that the recipient (or originator) of a cryptocurrency transaction could be a software protocol rather than an individual or business, let alone attempt to explain whether or how MSBs would be required to provide the "name and physical address" of a software protocol that is openly available for free online. The proposed rule leaves MSBs guessing as to whether and how they can process transactions with software protocols in a way that complies with the rule.

Even assuming compliance with the proposed rule were at least *theoretically* possible, for the Blockchain Association's obligated members to have any hope of accomplishing it, they would need to spend significant time and resources designing, building, and implementing new compliance infrastructure, which may be cost prohibitive. While the details concerning the costs and feasibility of compliance could not be assembled in 12 days over the holidays, it seems clear that, at a minimum, MSBs would likely have to design and build application programming interfaces to facilitate the collection of counterparty information at the point of transaction initiation (for outgoing transactions) or receipt (for incoming transactions). The NPRM does not indicate whether such a system would satisfy the proposed rule's requirements for counterparty identification. In addition to designing a system to proactively collect information about individuals with whom the MSBs have no relationship, MSBs would also likely need to build databases to store and protect transaction and counterparty information for five years after the transaction. To ascertain whether transactions are subject to the proposed requirements, MSBs would also have to be able to distinguish between cryptocurrency wallets held by individuals and those held by financial institutions. Newly collected counterparty information would presumably also have to be integrated into existing sanctions screening tools. While MSBs pursue this unpredictable and burdensome project, they would likely have to prohibit or substantially decelerate all transactions with subject wallet addresses, depriving their customers of expected services—and their property rights—for months or maybe even years.

Even if MSBs were able to develop a system to collect and report counterparty information to Treasury's unspecified satisfaction, the downstream burdens on MSBs offering services related to CVCs and LTDAs would be significant. When MSBs collect or receive additional information regarding the wallet address that customers are using for withdrawals and deposits, they would presumably be responsible for additional screenings (*e.g.*, Office of Foreign Asset Control (OFAC) sanctions, politically exposed persons (PEP), negative news, determination of the purpose and relationship of the transactions for AML review, etc.) that would significantly

aggravate the compliance costs of the proposed threshold reductions. These additional compliance costs would come in the form of vendor costs and person hours needed to not only manage the additional collection volume but also screen resulting alerts. Thus, even assuming MSBs *could* develop some means to comply with the proposed rule, doing so would likely be cost-prohibitive, leaving their customers unable to engage in any covered transactions at all.

4) The Proposed Rule Would Not Achieve Its Stated Law Enforcement Goals.

Not only would the proposed rule impose wholly impractical compliance burdens; it would do so in exchange for little if any law-enforcement value. The NPRM itself shows why.

While arguing that any comment period is a matter of administrative grace, the NPRM states that "undue delay in implementing this rule would encourage movement of unreported or unrecorded assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets, such as by moving CVC to exchanges that do not comply with AML/CFT requirements. Such delay presents an opportunity to illicit actors who have substantial proceeds in regulated financial institutions and who want to be able to move those funds without detection into the darker, unregulated corners of the CVC ecosystems …." 85 Fed. Reg. at 83,852. That statement is telling for at least two reasons.

First, it implicitly acknowledges that existing requirements have not prevented "illicit actors" from using the services of financial institutions and assembling funds in "hosted wallets at financial institutions." If existing rules have not prevented illicit actors from depositing "substantial proceeds in regulated financial institutions," then it is doubtful that a hastily promulgated extension of those rules will fare any better. What is required is thoughtful deliberation, not a hasty extension. Second, it is not "undue delay" in issuing the proposed rule that would encourage bad actors to move their assets to self-hosted wallets to avoid detection; it is gaps in the regulatory scheme itself that will remain unaddressed. All someone would need to do to ensure that their transactions would *not* be recorded or reported is keep their digital assets in a self-hosted wallet, as the proposed rule does not apply to transactions *between* self-hosted wallets. A self-hosted wallet thus can be used to transact with other self-hosted wallets, and it can be replenished from sources outside FinCEN's regulatory reach. At most, then, the proposed rule would just incentivize those who wish to keep their transactions private (whether for licit or illicit reasons) to keep their digital currency in a self-hosted wallet or in institutions beyond FinCEN's regulatory reach, thereby reducing the very transparency that FinCEN purports to be trying to foster.

5) The Proposed Rule Implicates Important Privacy Rights And Does Not Account For Risks to Americans' Data Security.

The proposed rule would enable the government to engage in an unprecedented level of surveillance of honest citizens' past, present, and future financial transactions that is anathema to free and open societies and implicates Fourth Amendment concerns. *See, e.g.*, *Carpenter v. United States*, 138 S.Ct. 2206 (2018) (recognizing limits to third-party doctrine in context of search of unprecedented location tracking data). Transparent blockchains immutably record cryptocurrency transactions on public ledgers, which are accessible and searchable by anyone with an internet connection. Requiring MSBs to associate blockchain addresses with individual citizens' identities thus would enable MSBs and the government to associate every single financial transaction ever made with a given blockchain address on a transparent blockchain with a specific individual. That would be akin to Treasury proposing a rule that would allow the government to see *every single cash transaction an individual has ever made or will ever make without first having to obtain a warrant*. What Americans spend money on reveals information

about every facet of their private lives, from political activity to health concerns. Surveillance power of this magnitude is precisely why authoritarian regimes like the People's Republic of China are eagerly pursuing a central bank digital currency that associates addresses with citizens' identities. The United States should not follow suit. Totally eliminating financial privacy for U.S. citizens just because they choose to use digital currency is not an acceptable or reasonable response to concerns about illicit financial activity. And it is certainly not a mere reporting requirement that should be imposed hastily and without express statutory authorization.

Associating public addresses with individuals' identities on transparent blockchains would also expose U.S. citizens to risk of surveillance by hostile actors, as the information MSBs must collect, record, and report under the proposed rule would be a prime target for cyber espionage. The proposal to create such an enticing "honeypot" of data is all the more disturbing given the recent hack of Treasury's own networks. In December 2020, Treasury suffered a "significant cyber incident" (*i.e.*, hack) that reportedly infiltrated all levels of Treasury's networks, including the email accounts of Treasury's top leadership. Department of Homeland Security, Joint Statement by the FBI, CISA, and the ODNI, Dec. 17, 2020, *available at* https://www.dhs.gov/news/2020/12/17/joint-statement-fbi-cisa-and-odni. Hacking is not the only risk that individuals face when Treasury collects their financial information: Earlier in 2020, there were unauthorized disclosures of reports submitted to FinCEN. *See* International Consortium of Investigative Journalists, *FinCEN Files*, *available at* https://www.icij.org/investigations/fincen-files/ (last visited Jan. 3, 2021). Those incidents and others demonstrate the potentially astronomical costs of aggregating troves of Americans' personal information. Such risks warrant intense scrutiny, not precipitous action.

FinCEN itself has acknowledged that the unauthorized disclosure of private financial information "can impact the national security of the United States, compromise law enforcement investigations, and threaten the safety and security of the institutions and individuals who file such reports." FinCEN, Statement Regarding Unlawfully Disclosed Suspicious Activity Reports, Sept. 1, 2020, *available at* https://www.fincen.gov/index.php/news/news-releases/statement-fincen-regarding-unlawfully-disclosed-suspicious-activity-reports. Yet the cost-benefit analysis presented in the NPRM does not recognize any of these serious costs to the American public and users of the U.S. financial system. Indeed, the NPRM lacks any discussion of risks the proposed rule would impose. Instead, the NPRM just punts to the general public the critical question of whether the proposal strikes "a reasonable balance between financial inclusion and consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity." 85 Fed. Reg. 83,851. Because FinCEN has failed to even consider the costs to and "burden on society" that would result from the proposed rule, FinCEN has necessarily failed to determine either that the proposed rule "maximize[s] net benefits" or that the proposed rule's "benefits justify its costs." *See* Executive Orders 13563; 12866.[1] That failure both violates Executive Orders 13563 and 12866 and reflects a lack of concern for Americans' privacy and financial security.

6) The Proposed Rule Would Stymie Innovation.

[1] The NPRM asserts that Executive Order 12866 is inapplicable because the NPRM "involves a foreign affairs function." Fed. Reg. 83,854. For the reasons described above, that reasoning is not likely to withstand a court challenge. To our knowledge, a new anti-money laundering regulation has never been promulgated under the guise of it being related to "a foreign affairs function" of the United States government. Money laundering is not a novel concern, and the NPRM fails to explain what makes the proposals at issue different from any other anti-money laundering rule.

The proposed rule also ignores the reality that blockchain public addresses have uses well beyond payments. While cryptocurrencies represent the primary application of blockchains right now, the potential applications are limitless. The fact that distributed ledgers are open to all allows anyone with an internet connection to experiment with them. Since the creation of the first cryptocurrency eleven years ago, innovators have explored a range of potential applications of blockchains, such as decentralized cloud storage networks and secure contracting.

Distributed ledgers can store unique data sets, including but by no means limited to a record of transactions in a given cryptocurrency. For example, one's public address and private key may be used to access a peer-to-peer network that stores files on the internet, *i.e.*, a decentralized "cloud storage" network. The types of data one could store via the use of decentralized networks are theoretically limitless, but an everyday example could be family photos or personal documents. An individual could use a private key managed with a self-hosted wallet to access these photographic or written digital "assets." Regulations applicable to financial transactions should have no application to those other uses of self-hosted wallets. Nor should the uses of such technology be stymied by the knowledge that government regulators can extend existing "reporting requirements" to such self-hosted wallets in ways that interact with the inherent nature of blockchain technology to give the government unprecedented access to heretofore private information. The chilling effect of such regulatory action is obvious.

Because the ecosystem is still in its infancy, as yet unimagined use cases for distributed ledgers will likely emerge. The blanket application of payments regulation to personal cryptocurrency wallets would not only fail to recognize the diverse applications (existing and potential) of distributed ledgers, but also stymie ongoing experimentation with distributed ledgers that could bring to fruition revolutionary products and services.

Conclusion

The Blockchain Association respectfully reiterates its request that the comment period for this NPRM be extended to at least 60 days. These comments reflect the Association's best efforts to assemble comments on a timeline that is simply incompatible with comprehensive data gathering, let alone fully deliberative comments. But even based on cursory data and truncated deliberation, the flaws of the NPRM are apparent. The Blockchain Association fully supports FinCEN's laudable goals of targeting money laundering, terrorism financing, and other illicit uses of CVCs or digital assets. But the proposed rule would do little if anything to advance them, and would impose severe costs on MSBs, owners of cryptocurrency, and the future of blockchain. FinCEN, Treasury, and the public would be better served by extending the comment period to ensure that both stakeholders and regulators can give these weighty matters the full and fair attention they deserve. Rather than rush to finalize a rule that suffers from deep procedural and substantive flaws, the comment period should be extended to allow for meaningful public comment on each of the topics detailed in the NPRM, so that FinCEN can craft an approach that will actually accomplish the government's important regulatory objectives without unnecessarily curbing innovation or treading on individuals' property and privacy rights.

Sincerely,

Kristin Smith
Executive Director

KIRKLAND & ELLIS LLP
AND AFFILIATED PARTNERSHIPS

1301 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
United States

+1 202 389 5000

www.kirkland.com

Paul D. Clement
To Call Writer Directly:
+1 202 389 5013
paul.clement@kirkland.com

Facsimile:
+1 202 389 5200

December 30, 2020

BY ELECTRONIC MAIL AND COURIER

Steven T. Mnuchin
Secretary of the Treasury
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets Convertible Virtual Currency NPRM

Dear Secretary Mnuchin:

I am writing on behalf of the Blockchain Association to respectfully request that you extend the extremely truncated notice and comment period for an extremely consequential proposed rule. Specifically, I am writing about the Financial Crimes Enforcement Network ("FinCEN") Notice of Proposed Rulemaking regarding "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "NPRM"). *See* 85 Fed. Reg. 83,840 (Dec. 23, 2020). The NPRM addresses one of the most complex and important issues in the blockchain and cryptocurrency realms, namely, the proper regulation of self-hosted wallets. Yet in tackling this difficult and momentous issue, the NPRM gives affected stakeholders, which the NPRM acknowledges are dispersed around the globe, just days to draft their comments and to try to assemble the supporting data. The NPRM underscores the complexity of the issues by identifying at least two dozen questions that need answering. Yet the NPRM would give stakeholders far more questions than days in which to answer them. To make matters worse, the brief comment period spans multiple federal holidays. With all due respect, this is no way to proceed on a subject this complicated and consequential. The highly truncated comment period sets up the government for failure on procedural grounds in the courts. But far more important in the long run, the breakneck speed at which the proposed rule is proceeding all but guarantees a substantively flawed final product. I therefore respectfully urge you to consider substantially extending the comment period to ensure that all interested parties—including the agency itself—will be able to engage in the kind of meaningful and productive dialogue that the Administrative Procedure Act is designed to foster and that this issue deserves.

The Blockchain Association is a not-for-profit organization dedicated to improving public policy in ways that will help blockchain networks and their users develop and prosper in the United States. Its diverse membership reflects the complexity of this dynamic market and includes projects building blockchain networks, trading platforms that allow users to exchange cryptocurrencies, and early stage investors that support the entire ecosystem. The Blockchain Association comprises industry leaders who are committed to responsibly building, funding, and supporting blockchain networks fueled by cryptocurrencies. It endeavors to educate policymakers, courts, and the public about how blockchain technology works and how regulatory clarity can bring about a more secure, competitive, and innovative digital marketplace. Given its diverse membership, the Blockchain Association is well positioned to provide FinCEN and the Department of the Treasury with the valuable perspectives of those who facilitate and engage in transactions involving convertible virtual currency or digital assets with legal tender status held in self-hosted wallets. And the Association and other members of the cryptocurrency community are eager to work with FinCEN and Treasury to help craft policies that accomplish the government's important regulatory objectives without unnecessarily curbing innovation or treading on individuals' property and privacy rights. But assembling diverse perspectives and achieving regulatory balance takes time. The rushed timeframe reflected in the current NPRM severely frustrates the Association's ability to provide vital input.

The timeframe reflected in the NPRM is entirely unrealistic given the nature of the issues and the reality of the calendar. Late in the day on Friday, December 18, 2020, FinCEN released a 72-page notice of proposed rulemaking that proposes the imposition of novel reporting and recordkeeping obligations on banks and money services businesses (or MSBs) with respect to transactions between the wallets they host and self-hosted wallets, or wallets with certain foreign financial institutions. The NPRM spans 72 pages, but its length still understates the difficulty and novelty of the issues. The NPRM seeks comments on 24 separately enumerated subjects and questions, some with multiple subparts. Yet the NPRM provides just 15 days to answer those 24 questions and to respond to the balance of the 72-page NPRM. And the NPRM does not even speak clearly or consistently about when that highly truncated comment period begins to run. Ordinarily, the comment period does not commence until publication in the Federal Register—here, December 23–which would result in a due date for comments of January 7, 2021. The published NPRM reflects that January 7 deadline in one place, 85 Fed. Reg. at 83,856, but sets an even more unforgiving January 4 deadline a few pages earlier, *id.* at 83,841. The Federal Register website says that all comments must be submitted by January 4, so the benefit of the doubt does not appear to go to the public. Instead, as best one can tell, the public has been given a 12-day window to submit comments over a major holiday period that includes Christmas Eve, Christmas (a federal holiday), New Year's Eve, New Year's Day (another federal holiday), and four weekend days. Some foreign countries in which stakeholders operate observe additional national holidays, and even the business days during this particular fortnight are a notoriously difficult time to locate anyone actually focused on business. That leaves interested members of

the public with, at best, a grand total of seven "working days" to comment on an NPRM that seeks feedback on more than three times as many topics. And on top of all that, efforts to submit comments have been frustrated by technical complications with the site (including error messages) on some of the few weekdays available for submitting comments.

The notion that stakeholders could meaningfully engage with a rule that touches on more than 24 separate subjects in such a highly truncated period would be doubtful even in the ordinary course. But it is wholly untenable in the context of an effort to impose sweeping new rules on a rapidly emerging and complex industry with which the government has very little regulatory experience. The novel nature of the government's regulatory exercise only heightens the need for robust participation by the many stakeholders in the still-nascent and evolving cryptocurrency industry. Yet the NPRM does not even give stakeholders all the information they need to provide the agency with meaningful comments, let alone give them the necessary time to compile that information. For example, roughly half of the topics on which FinCEN has expressly sought comment involve the potential costs of complying with the proposed reporting and recordkeeping requirements or with various alternative proposals. *Id.* at 83,851. But setting aside the problem that stakeholders did not learn of these proposals until shortly before close of business on the Friday before Christmas, the NPRM does not even purport to identify all the information it is proposing to require banks and MSBs to retain and report. *See, e.g.*, *id.* at 83,861 (proposing that requirements will *include* "[t]he 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*") (emphasis added). Commenting on the costs and burdens of reporting counterparty information is not feasible when the extent of the mandated information is a detail to be supplied later. Anyone who understands the cryptocurrency industry appreciates how critical such details are, as MSBs do not presently have (or even necessarily have the means to acquire) some or all of the counterparty information the Secretary may demand. FinCEN cannot seriously expect stakeholders to meaningfully assess, especially in seven business days, what it will cost to comply with regulatory obligations that have not yet been fleshed out.

Perhaps anticipating that this extraordinarily truncated comment period could not pass APA muster, the NPRM suggests that even this minimal nod to notice and comment is a matter of administrative grace, because FinCEN need not engage in any notice and comment at all. But the stated excuses for evading bedrock APA requirements will not withstand judicial scrutiny. The NPRM first posits that the rule implicates a "foreign affairs function," and so is exempt from notice and comment rulemaking entirely. *See id.* at 83,852; 5 U.S.C. §553(a)(1). But as the Administration was recently reminded, that a rule "implicates foreign affairs … is not enough to satisfy the foreign affairs function exception." *Capital Area Immigrants' Rights Coalition v. Trump*, 471 F. Supp. 3d 25, 56 (D.D.C. 2020). Instead, that narrow exception is satisfied only when a rule "clearly and directly involve[s] activities or actions characteristic to the conduct of

international relations." *Id.* at 53; *see also*, *e.g.*, *City of New York v. Permanent Mission of India to United Nations*, 618 F.3d 172, 202 (2d Cir. 2010). A rule that regulates wholly private financial transactions that may (or may not) involve foreign actors undoubtedly does not satisfy that demanding standard. Indeed, if the mere fact that financial transactions may involve foreign actors were enough to take a rule outside the APA, then Congress would not have needed to amend the Bank Secrecy Act to craft special procedures (not applicable here) that allow certain types of regulations of transactions with foreign entities to take temporary effect while notice and comment is ongoing. *See* 31 U.S.C. §5318A. As that limited and inapplicable exception reflects, it has long been settled law that the foreign affairs "exception cannot apply to functions merely because they have impact beyond the borders of the United States." *Mast Industries, Inc. v. Regan*, 596 F. Supp. 1567, 1581 (Ct. Int'l Trade 1984).

Nor would the APA's "good cause" exception apply here. *See* 5 U.S.C. §553(b)(3)(B). The good cause exception is "meticulous and demanding." *Sorenson Commc'ns Inc. v. FCC*, 755 F.3d 702, 706 (D.C. Cir. 2014). It is "narrowly construed and only reluctantly countenanced," with the agency bearing the burden of persuasion, and doing so without the benefit of any deference. *NRDC v. NHTSA*, 894 F.3d 95, 113-14 (2d Cir. 2018). The NPRM posits that "[u]ndue delay in implementing this rule would encourage movement of unreported or unrecorded assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets." 85 Fed. Reg. at 83,852. But the key phrase in that sentence is "*undue* delay." In circumstances where some notice and comment period is feasible, the APA determines that a delay for a period to allow for meaningful notice and comment is not just due, but legally required. By allowing even an extremely truncated comment period before the proposed rule takes effect, FinCEN has acknowledged this is not the rare situation where the rule must be imposed immediately to prevent circumvention. Where some comment period is viable, the APA demands a meaningful comment period, not 15 days over the holidays. And while the NPRM notes that "the prevention of substantial financial fraud" may constitute good cause, 85 Fed. Reg. at 83,853 (citing *Disabled in Action of Metro. New York, Inc. v. Brezenoff*, 506 F. Supp. 244, 248 (S.D.N.Y. 1980)), FinCEN has identified nothing even remotely comparable to the ongoing, multimillion-dollar fraud on a federal program that justified immediate agency action in *Brezenoff*.

The procedural problems with the NPRM will almost certainly result in the final rule being tied up in the courts and invalidated on procedural grounds. But the real problem with tackling such a novel and complex issue in such haste is that the rule that emerges from this rushed process will almost certainly be substantively flawed. The NPRM claims to target money laundering, terrorism financing, and other illicit uses of convertible virtual currency or digital assets. The Blockchain Association fully supports those laudable goals. But the proposed rule would do little if anything to advance them. Virtual asset service providers already maintain "know your customer" information and records of transactions for the customers whose wallets

they host. All the rule adds as a potential law-enforcement tool is a requirement that MSBs keep records of and report information regarding the holders of the self-hosted wallets or wallets hosted by certain foreign financial institutions with which their hosted wallet customers transact. It is not even clear that MSBs will be able to comply with those requirements, as MSBs do not typically have access to personal information about the holders of the self-hosted wallets with which their customers transact. Thus, what purports to be just a reporting requirement may well operate as a *de facto* ban. But even assuming MSBs can devise some means of compliance, the rule would have extremely limited utility, for all someone would need to do to ensure that their transactions would *not* be recorded or reported is keep their digital assets in a self-hosted wallet, which can be replenished from sources outside FinCen's regulatory reach, as the requirements do not apply to transactions *between* self-hosted wallets. At most, then, the rule would just lead those who wish to keep their transactions private (whether for licit or illicit reasons) to keep their digital currency in a self-hosted wallet, thereby reducing the very transparency that FinCEN purports to be trying to foster. That kind of mismatch between an agency's objectives and the means it has chosen for trying to accomplish them is exactly what a meaningful notice and comment process can identify and remedy.

There is a better way. Rather than rush to finalize a rule that suffers deep procedural and substantive flaws, there is still time to extend the comment period and invite meaningful public comment that will both eliminate the obvious procedural flaws and create the possibility for regulation that avoids the substantive difficulties of the approach reflected in the NPRM. The alternative of pressing ahead with an NPRM that raises dozens of questions, while providing stakeholders roughly half a dozen business days over the holidays to comment has nothing to recommend it. A rule produced by that flawed process will not survive court challenge and will not redress the problems the NPRM attempts to solve. In sum, FinCEN, Treasury, and the public would all be better served by extending the comment period to ensure that both stakeholders and regulators can give these weighty matters the full and fair attention they deserve.

Sincerely,

Paul D. Clement

cc: Jeffrey A. Rosen, Acting Attorney General of the United States
Kenneth A. Blanco, Director, Financial Crimes Enforcement Network
Russell Vought, Director, Office of Management and Budget