Stellar Development Foundation

292 Ivy Street Suite E
San Francisco, CA 94102
hello@stellar.org

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

Via Federal E-Rulemaking Portal: www.regulations.gov
and Via email: frc@fincen.gov

January 4, 2021

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

To Whom It May Concern:

The Stellar Development Foundation ("SDF") appreciates the opportunity to submit this comment letter for consideration by the Financial Crimes Enforcement Network ("FinCEN") with respect to the Notice of Proposed Rulemaking on "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "NPRM").[1] The NPRM's proposals have far-reaching consequences for the blockchain and cryptocurrency ecosystems and demand a thorough analysis by law enforcement, financial institutions, and the public. We note at the outset that this letter and, we suspect, the comment file as a whole, would have been more constructive and beneficial to FinCEN had the public been given a meaningful period of time to comment and we urge FinCEN to extend the comment period to 90-days.

SDF is a US-based nonstock, nonprofit organization that supports the development and growth of the Stellar network ("Stellar") and the "Stellar ecosystem" – the individuals, developers, and businesses who build on or interact with Stellar. Stellar is an open-source network that connects the world's financial infrastructure. Founded in 2014, SDF helps maintain Stellar's codebase, supports the technical and business communities building on the network, and serves as a speaking partner with policymakers, regulators, and institutions. Our mission is to create equitable access to the global financial system, using the Stellar network to unlock the world's economic potential through blockchain technology.

Stellar is a decentralized, fast, scalable, and uniquely sustainable network for financial products and services. It is both a cross-currency transaction system and a platform for digital asset issuance. Financial institutions worldwide issue assets and settle payments on the Stellar network, which has grown to over 4.7 million accounts.

[1] Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," *Federal Register,* 85 FR 83840 (December 23, 2020).

I. Introduction and the fiction of "unhosted" wallets.

SDF supports the mission of FinCEN to prevent and deter money laundering, the financing of terrorism, and other illicit financial activity. Preventing criminals and other bad actors from misusing blockchain technology and networks is good for society and good for the long-term growth and success of the blockchain industry. Stellar was built for compliance and includes key compliance functionality that enables businesses and developers building on the network to meet their compliance obligations. SDF is similarly committed to compliance and works with firms such as Elliptic, FinClusive, Sovrin, and Securrency to bring a suite of blockchain analytics, compliance-as-a-service, a Compliance and Inclusive Finance Rulebook, and other "regtech" tools to the Stellar ecosystem.[2] These tools and the nature of Stellar itself as a permissionless, public network frequently offer real time transparency, insights, and capabilities far beyond what is available in the traditional fiat world. We believe that these and other differences between blockchain architecture and fiat architecture warrant more thoughtful consideration of the best approaches to leveraging the unique nature of the technology and public, immutable blockchain ledgers in combating illicit activity involving convertible virtual currencies ("CVC").[3]

A deficiency of the NPRM is that it glosses over the important structural differences between the traditional fiat-based financial system and a reconceptualized blockchain-based system. The NPRM is an attempt to force an entirely new and different (decentralized) system into the regulatory structure built for the old (centralized) paradigm. Such an approach would forfeit the many benefits blockchain infrastructure can offer FinCEN and the broader law enforcement community while causing a number of unintended consequences. SDF encourages FinCEN to work with the blockchain industry to understand these benefits and then, if necessary, craft rules that enhance FinCEN's capabilities without unduly burdening the industry and its community of users.

This comment letter is intended to provide FinCEN with as much useful and actionable feedback as we are able given the truncated comment period that fell during the holidays. Specifically, we will address some of the most glaring procedural inadequacies with which this rulemaking has been proposed, we will highlight a number of troubling unintended consequences this rule would manifest if adopted, and finally, we will suggest a better approach to rulemaking in this area that would harness, rather than discard, the breakthroughs of blockchain technology.

A. There is no such thing as an "unhosted wallet."

As a permissionless, public network, most of the "wallets" that interact with Stellar are not "hosted" by a bank or money services business ("MSB") [collectively, "Bank Secrecy Act ('BSA') -regulated entities"] – a scenario which the NPRM has labeled "unhosted." The NPRM singles out such "unhosted" wallets for a substantial and adverse change in regulatory treatment, based on an assumption that unhosted wallets are primarily used for nefarious purposes. The proposed rule fails to define several key terms including

[2] SDF also participates in the Blockchain Alliance.

[3] We note that FinCEN's definition of CVC is overbroad, vague and ambiguous. It purports to define CVC in terms of other undefined terms (such as cryptocurrency) and includes anything short of legal tender capable of substituting for currency. Under this definition, CVC is not limited to digital assets – literally any object or property that can be traded could constitute CVC.

"wallet," "hosted," and "unhosted." This presents a significant opportunity for confusion which may impair the usefulness of the public comments received and the consideration thereof by FinCEN.

The NPRM's discussion of digital asset wallets reveals a misunderstanding of blockchain architecture that would benefit from additional public-private dialogue. The NPRM suggests that a digital asset wallet is a type of account maintained by a centralized intermediary. This perspective from FinCEN is reflective of the structure of traditional fiat-based finance. It also tracks the structure of digital asset wallets that are "hosted" by a BSA-regulated entity, but it exposes a fundamental misunderstanding of blockchain architecture.

At its core, a digital asset wallet consists of a public address or key that appears on a distributed ledger and a private key, which is closely held by the individual or entity with control over the assets attributed to that public address. These keys are unique strings of random characters. Custody and control over a wallet and its contents requires the private key, which can be as simple as a so-called "brain wallet" (committing the private key to memory), a "paper wallet" (writing it down on a piece of scrap paper), or a physical wallet (for example, inscribing it into some physical medium like stainless steel).[4] There are also technology solutions for private key management, including smartphone apps and physical hardware.

Just as in the fiat world, a digital asset owner may choose to entrust a third party with control over their assets. This is typically accomplished by sending the asset to a wallet controlled by the third party to hold on the sender's behalf. This appears to be what FinCEN means by the term "hosted wallet," though such term is not defined in the NPRM. Conceptually, this "hosted" digital wallet is no different from the account-based systems of banks with which FinCEN is so familiar. Such custodians, typically BSA-regulated entities, respond to orders from the account owner to, for example, withdraw the account balance or pay it to a third party. Although not defined in the NPRM, the term "unhosted wallet" appears to be anything capable of containing a private key (including a person's memory and scraps of paper) that is not an account maintained by a BSA-regulated entity. The term "unhosted" is misleading, however, as these wallets are not un-custodied, they are simply not custodied by an intermediary. They are custodied in the same way that a dollar bill in your back pocket, or a driver's license in your purse, or a gold coin in a home safe is custodied; that is to say that they are custodied directly by the owner. It is, therefore, more descriptive to refer to such self-custody arrangements as "self-hosted" than "unhosted," and so that is how we will proceed in this letter.

B. Self-hosted wallets are beneficial and necessary to the growth of the digital economy.

Just as in the fiat world, there are countless legitimate reasons why a person may choose to self-custody their digital assets.[5] Foremost among them is that many experts consider it to be the safest way to do so. Scores of cryptocurrency exchanges have been hacked, resulting in billions in losses.[6] While such criminal

[4] Whitehouse-Levine, Miller and Kelleher, Lindsey, Blockchain Association, *Self-Hosted Wallets and the Future of Free Societies* (November 2020), available at: https://theblockchainassociation.org/wp-content/uploads/2020/12/Self-Hosted-Wallets-and-the-Future-of-Free-Societies-01.pdf

[5] Ramaswamy, Jai, Coin Center, *How I Learned to Stop Worrying and Love Unhosted Wallets* (November 18, 2020), available at: https://www.coincenter.org/how-i-learned-to-stop-worrying-and-love-unhosted-wallets/.

[6] *See, e.g.*, https://www.ledger.com/academy/crypto/hacks-timeline.

activity may, in part, be FinCEN's motivation for proposing the NPRM, self-hosted wallets, and particularly users' ability to easily transact between self-hosted wallets and financial institutions like exchanges, is one of the most potent tools individuals have to protect themselves.

Individuals may also want to be accountable for their own funds, and may not trust a third party to keep an accurate and consistent ledger. The banking system in the United States is sound, but many countries have deep-seated issues that undermine trust in local governments and financial institutions. In those cases, a self-hosted wallet can provide users the assurance that their balances are tamper-proof because they are stored directly on an immutable and public record.

In many of the same places, self-hosted wallets remove barriers to entry to the financial world. According to the World Bank, there are 1.7 billion unbanked adults in the world, most of whom lack basic financial services because of the high costs associated with traditional bank accounts.[7] Self-hosted wallets, which are nearly free, give them an opportunity to hold funds and transact securely, which can help them access financial services and improve their material circumstances. In fact, self-hosted wallets benefit the entire payments ecosystem by encouraging efficiency and helping to keep costs low. As long as they are an option, institutions offering hosted wallets need to remain competitive, and so they're encouraged to streamline and innovate, which benefits consumers and improves the economy overall.

Additionally, self-hosted wallets allow users to reduce the number of intermediaries involved in transactions, especially in cross-border and cross-currency transactions. In the case of Stellar, users move money on and off the network by depositing funds with regulated financial institutions — a flow covered in more detail below — and those institutions collect necessary data including "know your customer" ("KYC") information before accepting a deposit or processing a withdrawal. Once a user has transferred funds onto the network using one of those regulated financial institutions, they can, using a self-hosted wallet, eliminate the need for additional intermediaries when making a remittance payment, which keeps consumer costs low and allows immediate settlement. The high costs of the current system of international payments, which are incurred because that system relies on a complex web of correspondent banks and other intermediaries,[8] can be sidestepped without sacrificing compliance.

II. The NPRM fails to meet the procedural requirements of the Administrative Procedures Act.

Our purpose in this comment letter is to address the substance of the NPRM; however, there are procedural failures with the NPRM that we feel are important to highlight. SDF is a member of the Chamber of Digital Commerce and the Blockchain Association, and SDF fully endorses their respective comment letters on this topic. With that said, certain aspects of the manner in which FinCEN has pursued this rulemaking create dangerous precedent if allowed to stand and, thus, bear repeating.

---

[7] The World Bank Group, *Global Findex Database* (2017), at 5.

[8] The World Bank Group, *Record High Remittances Sent Globally in 2018* (April 8, 2019), available at: https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018 (reporting banks were the most expensive remittance channel, charging an average fee of 11 percent of the amount remitted).

A. The unreasonably short public comment period and timing over the holidays appears to be a deliberate attempt to suppress public comment.

Section 553 of the APA states that "notice of proposed rule making shall be published in the Federal Register," and that after giving notice, "the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments." This requirement to give notice and an opportunity to be heard is the very essence of due process. The APA provides only very limited exceptions to this requirement, none of which apply to the NPRM.[9]

The NPRM was first announced after the close of business on Friday, December 18, 2020. It was not actually published in the Federal Register, the official commencement of the public comment period, until the following Wednesday, December 23, 2020. The comment period closed Monday, January 4, 2021. Inclusive of the 23rd and the 4th, that timeline allows a public comment period of only 13 calendar days.[10] Moreover, because those 13 calendar days span two federal holidays and two weekends, the public comment period includes just 7 business days. The NPRM contains 24 enumerated requests for comment and data (many of which contain multiple subparts), or more than three times the number of business days allotted to respond to them. Making matters worse, many people take additional days off from work and have heightened family obligations during the holiday period making communication and collaboration on responsive comments and data all the more difficult. Noting these challenges, courts have struck down rules that provided even longer comment periods simply because they fell over the holidays.[11]

---

[9] For a thorough analysis of the inapplicability of each exception to the APA's notice and comment requirement claimed by FinCEN in the NPRM, please see the following: (1) Section II of the comment letter submitted by the Chamber of Digital Commerce in response to this NPRM; (2) the letter from Perianne Boring and Amy Davine Kim of the Chamber of Digital Commerce to Treasury Secretary Steven T. Mnuchin dated December 22, 2020, available at: https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/Chamber-of-Digital-Commerce-Letter-to-Secretary-Mnuchin-c2.pdf; (3) the comment letter submitted by the Blockchain Association in response to this NPRM; (4) the letter from Paul D. Clement of Kirkland & Ellis LLP to Treasury Secretary Steven T. Mnuchin dated December 30, 2020, available at: https://theblockchainassociation.org/wp-content/uploads/2020/12/Blockchain-Association-Letter-re-Comment-Period.pdf; (5) the comment letter submitted by Coin Center in response to this NPRM, available at: https://www.coincenter.org/app/uploads/2020/12/2020-12-22-comments-to-fincen.pdf; and (6) the letter from eight Members of Congress to Treasury Secretary Mnuchin dated December 31, 2020, available at: https://www.coincenter.org/app/uploads/2020/12/Congressional-Letter-to-Treasury-123120-1.pdf.

[10] We note that this comment period is substantially non-compliant with Sec. 2 of Executive Order 13563, which states: "[r]egulations shall be adopted through a process that involves public participation. . . . To promote that open exchange, each agency, consistent with Executive Order 12866 and other applicable legal requirements, shall endeavor to provide the public with an opportunity to participate in the regulatory process. To the extent feasible and permitted by law, each agency shall afford the public a meaningful opportunity to comment through the Internet on any proposed regulation, *with a comment period that should generally be at least 60 days*" (emphasis added).

[11] *See*, *Pangea Legal Servs. V. United States Dep't of Homeland Security*, No. 20-cv- 07721, 2020 WL 6802474, (N.D. Cal. Nov. 19, 2020), ("thirty days for a rule of this magnitude . . . is already short. That the comment period spanned the year-end holidays shortened the period further still and undercut the purpose of the notice process to invite broad public comment.").

While the APA does not set a minimum period for comment, courts applying the APA have found that "exceedingly short" comment periods do not "provide a meaningful opportunity for comment."[12] Only in "rare" instances "actually warranting" a shortened comment period will a comment period as short as this one be permitted.[13] Rather than responding to an emergency situation, the NPRM appears to be a so-called "midnight regulation" that is being rushed due to the impending change of administration.[14]

We experienced the challenges this timeline presented when we tried to confer with a member of the Stellar ecosystem that is a registered MSB on the NPRM's impact on their business. Such firsthand information would undoubtedly be valuable to FinCEN, especially in performing the industry burden analysis and estimating the volume of new currency transaction reports ("CTRs") FinCEN would receive. However, we were unable to collect this information, because the principals of that MSB were already out of the office for the holidays. Of course, FinCEN was fully aware of this timeline and the complications it would cause upon releasing the NPRM and prescribing such a short comment period over the holidays.

B. FinCEN's invocation of emergency and foreign affairs exceptions under the Administrative Procedures Act are not supported by law or fact.

FinCEN claims that two exceptions to the APA notice and comment requirement, namely the "Foreign Affairs Exception" and the "Good Cause Exception,"[15] excuse it from the requirement, but they have nevertheless *chosen* to seek public comment.[16] However, FinCEN offers little support for the applicability of these exceptions to the NPRM, and reliance here renders the requirements of the APA meaningless. Any future proposal that could establish a nexus to financial transactions with individuals outside the U.S. or illicit activity would skirt the public comment requirement.

Beginning on page 83853 of the Federal Register, FinCEN argues that the APA's Foreign Affairs Exception applies "whenever a foreign affairs function [of the U.S. government] is 'involved.'" FinCEN asserts that the Foreign Affairs Exception is satisfied when, in FinCEN's opinion, "a foreign financial institution is not subject to adequate AML/CFT regulation," or when "individuals outside the United States transact without using a financial institution."[17] Were the threshold to meet the Foreign Affairs Exception truly this low, any colorable foreign consequence of a proposed rule would excuse the proposing agency from the APA. With its focus on preventing money laundering and the financing of terrorists, seemingly any rule proposed by FinCEN or any other agency under the BSA would be *prima facie* exempt from the APA.

FinCEN also cites the applicability of the Good Cause Exception, which generally applies to emergency situations where providing for notice and comment would itself cause greater public harm than the harm

---

[12] *N. Carolina Growers' Ass'n, Inc. v. United Farm Workers*, 702 F.3d 755, 770 (4th Cir. 2012).
[13] *Id*.
[14] Hunnicut, Trevor, Reuters, *Biden to act quickly to roll back harmful 'midnight regulations' -transition* (December 30, 2020), last accessed January 4, 2020 at: https://www.reuters.com/article/us-usa-biden-transition/biden-to-act-quickly-to-roll-back-harmful-midnight-regulations-transition-idUSKBN29422E.
[15] *See supra* note 9.
[16] NPRM at section VI.
[17] NPRM at 83853.

of denying the public its right to meaningful participation in the process.[18] FinCEN asserts that "undue delay in implementing this rule" would harm the public, because "malign actors may exploit such a delay by moving assets to unhosted wallets and away from regulated financial institutions."[19] However, these transactions are not new or emerging, nor does the NPRM prevent nor prohibit them, it simply imposes new reporting and record-keeping requirements about them. To the extent that this risk is either new or exigent, it is due to FinCEN's publication of the NPRM. FinCEN's decision to allow a public comment period gave "malign actors" more than enough time to move their assets, which takes minutes or hours, not days or weeks. Once created, the risk would not have been substantially increased by extending the public comment period to the more typical 60 or 90 days. Allowing for a more meaningful comment period would have helped balance FinCEN's self-created risk.

FinCEN's second justification for the Good Cause Exception references "concerns about national security, terrorism, ransomware, money laundering, and other illicit financial activities,"[20] citing illicit conduct dating back to June 2017[21] - thus undermining any claim of exigency. While stemming this type of criminal and illicit activity always demands a degree of urgency, the APA requirements would be rendered meaningless if the "Good Cause Exception" were applied to any situation with a nexus to illicit activity. FinCEN offers no specific evidence of how this illicit activity will be exacerbated by providing adequate time for meaningful input from law enforcement, financial institutions, and members of the public, all of whom have important voices, roles, and perspectives in preventing it.

FinCEN's interpretations of both the Foreign Affairs Exception and the Good Cause exception are clearly inconsistent with a large and well-settled body of case law under the APA.[22] If FinCEN's interpretation of the APA exceptions were correct, notice and comment under the APA would largely become a voluntary exercise by federal agencies, not the statutory mandate that it is. With neither of its claimed exceptions available, the NPRM is subject to the full notice and comment requirements of the APA. On the basis of these procedural violations alone, the NPRM should be withdrawn.

//

//

---

[18] *Mack Trucks, Inc. v. E.P.A.*, 682 F.3d 87, 95 (D.C. Cir. 2012) ("The question is not whether dispensing with notice and comment would be contrary to the public interest, but whether providing notice and comment would be contrary to the public interest.").

[19] NPRM at 83853.

[20] NPRM at 83852.

[21] NPRM at 83842, footnote 16.

[22] *See, e.g.*, *Invenergy Renewables LLC v. United States*, 422 F. Supp. 3d 1255, 1289 (Ct. Int'l Trade 2019) ("The foreign affairs exception, like all similar exceptions to the APA's notice-and-comment requirements, is quite narrow."); *City of New York v. Permanent Mission of India to United Nations*, 618 F.3d 172, 202 (2d Cir. 2010) (The phrase "foreign affairs function" should not be interpreted loosely "to mean any function extending beyond the borders of the United States."); *E. Bay Sanctuary Covenant v. Trump,* 932 F.3d 742, 775 (9th Cir. 2018) ([This exception] "requires the Government to do more than merely recite that the Rule 'implicates' foreign affairs."); *Am. Ass'n of Exporters & Importers-Textile & Apparel Grp. v. United States*, 751 F.2d 1239, 1249 (Fed. Cir. 1985) (quoting H. Rep. No. 1980, 69th Cong., 2d Sess. 23 (1946)); and *Rajah v. Mukasey*, 544 F.3d 427, 437 (2d Cir. 2008) ("For the exception to apply, the public rulemaking provisions should provoke definitely undesirable international consequences.").

III. The NPRM's regulatory impact analysis disregards applicable requirements and would not withstand judicial review.

The NPRM contains only a cursory attempt at a regulatory impact analysis which does not meet the requirements of Executive Order ("EO") 12866, EO 13563 and Office of Management and Budget ("OMB") Circular A-4.[23] EO 13563 begins with the admonition that "[o]ur regulatory system must . . . identify and use the best, most innovative, and least burdensome tools for achieving regulatory ends. It must take into account benefits and costs, both quantitative and qualitative,"and continues that, "[i]n applying these principles, each agency is directed to use the best available techniques to quantify anticipated present and future benefits and costs as accurately as possible." EO 12866 is even more explicit, stating " [f]ederal agencies should promulgate only such regulations as are required by law, are necessary to interpret the law, or are made necessary by compelling public need . . . In deciding whether and how to regulate, agencies should assess all costs and benefits of available regulatory alternatives, including the alternative of not regulating," and that "in choosing among alternative regulatory approaches, agencies should select those approaches that maximize net benefits . . ."

On its face, the NPRM did not adhere to these principles. In most cases, it failed to consider the factors identified in EO 12866. In many instances, there is simply not enough information in the NPRM to determine whether and to what extent FinCEN complied with EO 12866. This may be because, as with respect to its obligations under the APA, FinCEN summarily absolved itself of compliance with EO 12866 by claiming the NPRM "involves a foreign affairs function."[24] However, as we and others have forcefully contended, FinCEN is not entitled to rely on the Foreign Affairs Exception with respect to the NPRM and, therefore, is fully subject to the requirements of EO 12866.[25] We note that FinCEN has also failed to comply with EO 13771, a requirement that an agency repeal at least two existing regulations for each new regulation promulgated.[26]

Because the philosophies, principles, and requirements set out in EO 12866 and OMB Circular A-4 are so extensive, the OMB Office of Information and Regulatory Affairs ("OIRA") published an extensive checklist for agencies undertaking a regulatory impact analysis ("RIA").[27] The OIRA checklist guides agencies through the rigors of the RIA process via a series of detailed prompts and questions covering everything from a description of the need for the regulatory action and a cost-benefit analysis, to the impacts on disadvantaged and vulnerable populations.[28]

---

[23] Executive Order 13563, *Improving Regulation and Regulatory Review* (January 18, 2011), available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/eo12866/eo13563_01182011.pdf; Executive Order 12866, *Regulatory Planning and Review* (September 30, 1993), available at: https://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf; Office of Management and Budget Circular A-4, *Regulatory Analysis* (September 17, 2003), available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/regulatory_matters_pdf/a-4.pdf.

[24] NPRM at 83854.

[25] *See supra* note 9.

[26] NPRM at 83855, where FinCEN again summarily excuses itself from complying with EO 13771 by claiming the NPRM involves a "national security function" while providing no legal or evidentiary basis to substantiate this claim.

[27] Office of Information and Regulatory Affairs, *Agency Checklist: Regulatory Impact Analysis*, available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/regpol/RIA_Checklist.pdf.

[28] *Id*.

An evaluation of the NPRM's RIA yields primarily negative answers to most of OIRA's questions. For example, the NPRM's RIA includes no baseline, no accounting statement, no cost-benefit table, no analysis of effects on disadvantaged populations, and, as we'll explore more in the next section, no real attempt to quantify or monetize the anticipated costs and benefits of the proposed rule.[29]

A. The regulatory impact analysis present in the NPRM is arbitrary and capricious.

The NPRM's RIA fails to address the questions on OIRA's checklist. It includes only one cost estimate and no benefit estimate. Its evaluation of alternatives includes only slight variations on the rule as proposed. And, it provides no justification for a number of critical assumptions.

For example, the NPRM identifies two figures containing a number of embedded assumptions to arrive at "a reasonable minimum estimate for the burden of administering this rule."[30] FinCEN estimates the primary cost of complying with the proposed rule is 1,284,349-burden hours at $24.00 per hour for a total cost of $30.8 million annually.

The number of burden hours comes from the NPRM's Paperwork Reduction Act ("PRA") analysis beginning at page 83856. FinCEN estimates that 10,907 financial institutions will be subject to the NPRM, consisting of all banks, all credit unions, and an unidentified subset of MSBs. FinCEN does not disclose how or why it included some MSBs but not others. Next, FinCEN estimates that the annual compliance burden of the NPRM on banks and credit unions will be just one hour per year. Then, to calculate the time burden on MSBs, FinCEN simply repurposed the burden-hour estimates it used for an unrelated rulemaking, its previous "Funds Transfer/Travel Rule NPRM," without explanation of how these two rules might result in equal compliance burdens. These estimates do not represent a good faith effort to quantify the actual cost of compliance and are yet another example of how FinCEN's rushed process has failed to gather accurate and relevant information from the affected entities in the private sector. It may be that those assumptions are reasonable, but before that conclusion can be reached, FinCEN must provide a detailed and rigorous explanation informed by those who actually perform these compliance functions.

Further complicating the determination of an accurate estimate of burden hours, FinCEN omitted necessary variables. For example, no draft or mockup of the reporting form that covered entities will be required to file with FinCEN is included in the NPRM. So, neither FinCEN nor the public can accurately estimate the amount of time it would take a covered entity to gather the necessary information and process the filing. Moreover, these forms shall include "the name and address of each counterparty, *and such other information as the Secretary may require*" (emphasis added).[31] Without more specificity of the requirements of the form, estimates of the compliance burden will necessarily be inaccurate.

---

[29] We note that the United States Court of Appeals for the District of Columbia has set a high bar for agency cost-benefit analysis. *See, e.g.*, *Business Roundtable v. SEC*, 647 F.3d 1144 (D.C. Cir. 2011); *American Equity Investment Life Insurance Company v. SEC*, 613 F.3d 166 (D.C. Cir. 2010); and *Chamber of Commerce v. SEC*, 412 F.3d 133 (D.C. Cir. 2005).

[30] NPRM at 83854.

[31] NPRM at 83860.

Similarly, when it comes to assigning a cost to each burden hour, FinCEN simply repurposes its assumed $24/hour average labor cost of storing SARs prepared in response to its OMB control number renewal.[32] Why is it reasonable to assume that the average labor cost for storing SARs will be the same as the average cost of the compliance functions required under the NPRM? Why is the analysis performed for the OMB control number renewal a valid proxy for the NPRM? These questions are not answered. Finally, the NPRM acknowledges other sources of cost that it failed to consider entirely, such as "information technology implementation costs" which it admits are likely to be "non-trivial."[33]

The purported benefit of the proposed rule is "enhanced law enforcement ability to investigate, prosecute and disrupt the financing of international terrorism and other priority transnational security threats, as well as other types of financial crime, . . ."[34] But, when it comes to quantifying and monetizing this anticipated benefit, the NPRM does not even try. It simply states "[t]he cost of terrorist attacks can be immense." The NPRM admits that "[o]f course, it is difficult to quantify the contribution of a particular rule to a reduction in the risk of a terrorist attack," but nevertheless concludes that "even if the proposed rule produces very small reductions in the probability of a major terrorist attack, the benefits would exceed the costs."[35] The NPRM presents no basis for these conclusory statements. The NPRM offers no evidence of causality or even correlation between self-hosted wallets and terrorist attacks on the U.S. Further, it offers no support for the proposition that the NPRM's self-hosted wallet recordkeeping and reporting requirements would in any way reduce the frequency or severity of terrorist attacks on the U.S. Based on the information presented in the NPRM, any connection between self-hosted wallets and terrorist attacks against the U.S. is pure speculation. As with the cost assumptions discussed above, it may be that evidence to support these alleged benefits exists – that is not for this commenter to decide. But, what is clear, is that FinCEN has not done enough to gather, evaluate and present such analysis as it is required to do under applicable administrative procedures.

B. The NPRM fails to consider other significant costs.

As EO 12866 and EO 13563 make clear, an agency must consider the costs of a proposed regulation not only on the regulated entities, but also on individuals and society as a whole.[36] The NPRM does not attempt to identify, much less quantify, such costs. While not incumbent upon commenters to perform this analysis for FinCEN, a few individual and public costs are readily apparent and will be explored in more detail in the sections to follow. In no particular order, a non-exhaustive list of costs not considered by FinCEN with respect to the NPRM includes:

- The loss of individual privacy and the costs on individuals and society of heightened financial surveillance by both public and private sector entities;
- The increased risk to individuals of becoming victims of cybercrime as a result of leaks, hacks or other data breaches of reported financial data collected by financial institutions and government agencies, including:
    - Identity theft and fraud,

[32] NPRM at 83854.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] EO 13563(1)(b)(2) and EO 12866(1)(b)(11) ("Each agency shall tailor its regulations to impose the least burden on society, including individuals, . . .").

    - Phishing,
    - Ransomware,
    - Burglary, and
    - Extortion and other physical threats;
- The costs of reduced financial access and inclusion on disadvantaged or vulnerable populations, e.g., as a result of "de-risking;"
- The increased risk to society of financial censorship and to individuals and businesses of "de-platforming;"[37]
- The opportunity costs of lost, forfeited or otherwise suppressed economic activity and job creation, e.g., from entrepreneurial and other innovative activity fleeing from or avoiding the U.S. in favor of more welcoming regulatory jurisdictions; and
- The cost to society in terms of reduced global competitiveness and national security in a "critical and emerging technology."[38]

C. The NPRM fails to adequately consider less costly and less intrusive alternatives.

The NPRM purports to consider five "alternatives" to the proposed rule.[39] However, each of these "alternatives" is merely a slight tweak or variation of a component of the rule as proposed. In other words, the NPRM does not consider any *conceptual* alternatives to its proposal. For example, one conceptual alternative FinCEN could have considered was a regulatory regime making greater use of blockchain analytics in place of a bulk data collection scheme, but it did not do so. Additionally, the NPRM gave no consideration to the alternative of not regulating, as required by EO 12866(a). Of the five "alternatives" considered, only one would arguably have been less intrusive than the rule as proposed, a theme repeated in the NPRM's enumerated requests for comment in which FinCEN clearly contemplates an even more burdensome and intrusive regulatory scheme.[40]

The discussion of each of the five alternatives identified is a mere paragraph, which fails in each case to quantify the alternative's relative costs or benefits and ultimately fails to explain why the alternative chosen is the least burdensome, the most cost-effective, and maximizes net benefits.

//

//

//

[37] *See, e.g.*, Office of the Comptroller of the Currency, Notice of Proposed Rulemaking OCC-2020-0042, *Fair Access to Financial Services*, 85 FR 75261 (proposed rule to prohibit banks from refusing to serve legal but unpopular businesses). Similar risks are raised at the individual level given the granularity and attribution of the data the NPRM would collect.

[38] *Infra* note 58. Distributed ledger technologies were identified as a "critical and emerging technology" by the National Security Council in October 2020.

[39] NPRM at 83854.

[40] *E.g.*, the potential requirement to verify the identity of all of a financial institution's customer's counterparties at Requests for Comment (15) and (21).

IV. The NPRM will fail to deliver on its stated objective and will, instead, cause significant adverse unintended consequences.

A. The NPRM will complicate and frustrate law enforcement investigations involving convertible virtual currency.

While the NPRM's stated goal is to help combat illicit activity, we are concerned that its reporting and record-keeping requirements might have the opposite effect by driving illicit activity further away from the reach of law enforcement. The Department of Justice ("DOJ"), Office of the Inspector General's ("OIG") December 2020 Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities[41] highlights the connection between the use of the dark web and CVCs for illicit transactions across virtually all areas of capital driven illicit activity.[42] According to DOJ, "the existence of darknet marketplaces is one of the greatest impediments to [DOJ's] efforts to disrupt cybercriminal activities."[43] We believe that the NPRM's reporting requirements may exacerbate the challenges presented by darknet marketplaces by creating further incentives for criminals to avoid using regulated entities in favor of less transparent platforms and/or institutions not subject to the NPRM. This would drive their activities further into the "dark" by removing visibility into the peer-to-peer markets that currently exist thanks to the interaction between regulated, hosted wallets and self-hosted wallets. Rather than trying to wall them off from each other as would the NPRM, FinCEN should be seeking ways to further leverage these touchpoints to maximize its ability to gather useful law enforcement data.

Even if the NPRM's requirements do not drive bad actors into the dark, the NPRM fails to evaluate whether its proposals would create more useful reporting or simply more reporting. For example, we note that the NPRM offers no evidence that the additional CTRs required by the NPRM would necessarily improve law enforcement's ability to disrupt illegal activity. Similarly, the NPRM cites the large number of suspicious activity reports ("SARs") filed regarding CVCs,[44] but fails to indicate whether these reports a) have all been analyzed and acted upon by law enforcement or b) have led to an increased number of apprehensions. As reported by Buzzfeed News on September 20, 2020, "FinCEN received more than 2 million SARs last year. That number has nearly doubled over the past decade, as financial institutions have faced mounting pressure to file and the volume of international transactions has grown. Over the same period, FinCEN's staff has shrunk by more than 10%. Sources there say most SARs are never even read, let alone acted upon."[45] We would expect FinCEN's proposed requirement for increased and burdensome reporting to be supported by evidence that such reporting is valuable and effective in addressing the stated goal of combating illicit activity. Without such supporting evidence, we fear the effect of the NPRM will be that BSA-regulated entities will expend significant time and resources on reporting and filing CTRs on lawful transactions by law-abiding citizens without any significant increase in valuable law enforcement data.

---

[41] U.S. Department of Justice, Office of Inspector General, *Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities* (December 2020), available at: https://oig.justice.gov/news/doj-oig-releases-report-fbis-strategy-and-efforts-disrupt-illegal-dark-web-activities.

[42] *Id*. at 32.

[43] *Id*. at (i).

[44] NPRM at 83842, footnote 14 and accompanying text.

[45] BuzzFeed.News, *The FinCEN Files* (September 20, 2020), last accessed December 29, 2020 at: https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks.

An alternative approach might be to work with BSA-regulated entities, blockchain analytics companies, and law enforcement to devise more targeted approaches to identify illicit uses of CVCs and to refine suspicious activity reporting in the context of blockchain transactions. Blockchain ledgers provide an unprecedented level of transparency and traceability for transactions that is unparalleled in the fiat world. Blockchain analytics companies have developed tools and techniques that enable the monitoring and tracking of suspicious financial activity with a rich transaction history. Such traceability can empower regulated entities to better identify bad or suspicious actors before engaging with them and can assist law enforcement in establishing attribution for actors who use a combination of hosted and self-hosted wallets. Indeed, a review of the successful law enforcement actions cited in the NPRM and DOJ's recent Cryptocurrency Enforcement Framework[46] to determine how many of the investigations benefited from the alleged offender(s)' use of both hosted and self-hosted wallets might offer valuable insights into the wisdom of a rule that would incentivize bad actors to move away from regulated service providers, with accessible attribution information, to less transparent platforms.

B. The NPRM will create new cybersecurity and privacy risks for the public that outweigh any law enforcement benefit.

SDF is also concerned about the NPRM's increase in government-mandated collection of information about law-abiding Americans and the attendant increase in risk to which it would expose them. The NPRM would require a dramatic increase in the collection and reporting of sensitive financial information, including personally identifiable information ("PII") of parties and counterparties to transactions, to FinCEN, without adequate support for the law enforcement benefit, if any.

It is also critical to note the unprecedented scope of information FinCEN would have regarding blockchain transactions. Unlike the fiat banking system, where the details of an individual's transactions are closely guarded by custodial institutions, anyone can view all transactions associated with a public address on a blockchain. Once a public address is attributed to an individual, her transaction history can be reconstructed and future transactions can be traced. Because of this transparency, by combining information contained in CVC transaction reports including the name, physical address, and blockchain address of the customer *and* the counterparty, FinCEN will be able to construct a constantly updating map of public address owners and would then be able to track every transaction those wallet owners have ever made and will ever make, whether below or above the reporting and recordkeeping thresholds, and whether before or after the effective date of the rule. By comparison, in the traditional system, a CTR provides information limited to the transaction in question, the account holder and account number at a particular moment in time and no more. It does not unlock visibility into all of the account holder's transactions, at least not without a legal basis to obtain a subpoena or search warrant for such additional information.

The scale of this intrusion on privacy cannot be overstated – it includes not only the information related to the institution's customer and the transaction at hand, but also to every transaction that each *counterparty* makes both before and after the subject transaction. This vastly exceeds the amount of information the government currently has the right or ability to obtain with respect to fiat transactions. To

[46] U.S. Department of Justice, *Cryptocurrency Enforcement Framework* (October 2020), available at: https://www.justice.gov/ag/page/file/1326061/download.

lay this out more clearly, this means that a counterparty to a transaction, who has no relationship with the bank or MSB and has not consented to the collection and disclosure of its private information, could have its identity and entire wallet history and future transactions exposed to both that financial institution and the government in perpetuity based on the receipt of a transaction that subjects the *sender* to the aggregated CRT reporting requirements of the NPRM. This is an extraordinary expansion of the amount of information provided to third parties about customers and non-customers alike.

The NPRM also floats the idea of requiring verification of a covered institution's customer's counterparties at Requests for Comment (15) and (21). Such a requirement would be a dramatic departure from existing regulatory requirements applicable to BSA-regulated entities with respect to fiat transactions, neither of which typically conduct counterparty verification in the absence of a specific red flag. It is also unclear how BSA-regulated entities would accomplish such verification as a practical matter, since those entities would not have a relationship with the counterparty, who would be under no obligation to provide it. It would also present a significant burden on consumers who may be repeatedly asked to submit to verification by multiple financial institutions with which they have no relationship.

Such a reporting and verification regime could easily spell the end of financial privacy for blockchain users. We believe most Americans would view the government's ability to track every financial transaction they make without appropriate legal process as a shocking invasion of privacy. While there are good reasons to report certain transactions to the government, such as when suspicious activity is detected, enabling such granular tracking of the real-time financial activities of individuals who are under no suspicion of wrongdoing surely cannot be justified even in a situation where the additional reporting is likely to be of significant help to law enforcement (which as noted before, is the not case with respect to the NPRM). The Fourth Amendment is clearly implicated here, and yet, the NPRM fails to address these concerns at all. Its only mention of consumer privacy whatsoever comes at Request for Comment (4), wherein it asks "Has FinCEN struck a reasonable balance between financial inclusion and consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity?" It has not. Before proceeding with the proposed Rule, FinCEN should publish a thorough explanation of the constitutionality of its proposed action.

The NPRM would also create significant new cybersecurity risks for individuals. In addition to FinCEN or other government actors, the individual BSA-regulated entities required to gather and retain PII from CVC customers and their counterparties could also create similar wallet-identity maps of their own. It is not hard to imagine the many creative and intrusive ways the private sector might seek to monetize this data. But the far greater concern is that the required increase in the collection and retention of PII coupled with financial information will create giant troves of valuable data across both government agencies and BSA-regulated entities. Inevitably, this will increase both the frequency and severity of hacks, data breaches, and leaks.

Examples of large-scale data breaches are not limited to the private sector. One need look no further than the recent "SolarWinds breach" which compromised the systems of over 18,000 organizations including the Treasury Department, at least seven other cabinet-level departments of the federal

government, and most Fortune 500 companies.[47] The full extent of the entities compromised and the data stolen or manipulated remains unknown. FinCEN itself recently compromised the PII of individuals through a leak of over 2,500 sensitive documents, including over 2,000 SARs.[48] By FinCEN's own admission, the leak "threaten[ed] the safety and security of the institutions and individuals who file such reports."[49] In August 2017, the Securities and Exchange Commission acknowledged that its EDGAR filing system had been breached, allowing the attackers to profit from non-public information.[50] Examples of similar breaches in the private sector are too many to name.

While we appreciate the importance of providing timely, accurate, *and useful* information to law enforcement, that goal must be weighed against the importance of protecting the security and privacy of citizens. If these organizations cannot safeguard the sensitive information with which they have already been entrusted, the solution cannot be to give them more. This concern is even more acute in the context of blockchain networks for the reasons previously discussed. If, as the NPRM would require, financial institutions and governments agencies with track records of system vulnerabilities collect and retain (1) personally identifiable information including (2) physical addresses, and financial transaction data including (3) asset amounts and (4) wallet addresses, then they would become virtual goldmines for hackers and cybercriminals who, once in possession of this information, would have everything they need to attack those individuals either virtually or physically. FinCEN should not pursue policies that put consumers at greater risk of cybercrime.

C. The NPRM will impair the ability of blockchain technology to reach un- and underbanked populations and may increase such populations by encouraging "de-risking."

Section I.A of the NPRM acknowledges that "Blockchain-based CVC networks present opportunities as well as risks," and quotes the G7 Finance Ministers and Central Bank Governors, who note that "[t]he widespread adoption of digital payments [such as CVC] has the potential to address frictions in existing payment systems by improving access to financial services, reducing inefficiencies, and lowering costs."[51] What the NPRM fails to consider is that a robust ecosystem of self-hosted wallets is vital to realizing those benefits.

According to a 2019 Federal Reserve report, 22% of adults in the U.S. are unbanked — meaning that they have neither a savings nor a checking account — or underbanked — meaning that they rely on expensive

---

[47] The New York Times, *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit* (December 14, 2020), last accessed December 30, 2020 at: https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

[48] BBC News, *FinCEN Files: All you need to know about the documents leak* (September 21, 2020), last accessed December 30, 2020 at: https://www.bbc.com/news/uk-54226107; *see also supra* note 45.

[49] FinCEN, *Statement by FinCEN Regarding Unlawfully Disclosed Suspicious Activity Reports* (September 1, 2020), last accessed December 30, 2020 at: https://www.fincen.gov/news/news-releases/statement-fincen-regarding-unlawfully-disclosed-suspicious-activity-reports.

[50] U.S. Securities and Exchange Commission, *SEC Chairman Clayton Issues Statement on Cybersecurity* (September 20, 2017), last accessed December 30, 2020 at: https://www.sec.gov/news/press-release/2017-170.

[51] NPRM at 83842, footnote 11 and accompanying text.

alternative financial services to get by.[52] According to the World Bank, there are 1.7 billion unbanked adults worldwide.[53] The primary reason so many people suffer from lack of access to financial infrastructure is that traditional financial institutions are profit-driven and, therefore, avoid relationships with whole swaths of the population they deem unprofitable to serve. Rather than managing the risks associated with offering services to those who are poor, have insufficient credit history, or lack acceptable documentation, financial institutions often choose to "de-risk" by denying them access altogether.

Blockchain can solve the problems of inequitable access to financial infrastructure by offering an efficient public ledger that allows ownership and conversion of value without the prohibitive costs charged by incumbent intermediaries. It can do so by giving individuals control over their own money and the ability to transact in a nearly fee-less environment, and it can do it in a way that still allows financial institutions to exercise necessary due diligence. To understand this point, let's look at a specific example: how Stellar creates a new infrastructure to improve cross-border remittance payments.

Each year, over $500 billion of value is transferred cross-border through personal remittances. In most cases, remittances are transfers of money from foreign workers to family members in their home country. As part of its 2030 Agenda for Sustainable Development, the United Nations set a goal "to reduce to less than 3 per cent the transaction costs of migrant remittances and eliminate remittance corridors with costs higher than 5 percent."[54] However, current sending costs can be as high as 15% when transferring money to people in developing economies. These high costs are a result of the current web of intermediaries necessary to connect siloed payment systems, and are borne by those who can afford them least.[55]

Stellar was designed to solve the problems associated with current remittance infrastructure by connecting disparate payment systems on a single platform. It allows regulated financial institutions to serve as network on/off ramps by issuing digital assets on a public blockchain. Users deposit fiat currency with these institutions in return for a digital equivalent of that currency — tokens — and can redeem those tokens with the issuing institution for the underlying asset they represent. When a user makes a fiat deposit or withdrawal, the institution complies with local regulations, collecting KYC and any other required information. Users move value on or off the network through one of these regulated financial institutions.

However, once a user has value on the network, they can take advantage of Stellar's built-in orderbooks that facilitate conversion of currencies to send payments that originate in one currency, and arrive at their destination as another. Because the network is distributed and public — and therefore not owned by any one entity — the fee for a transaction is miniscule. Because the technology is efficient, a cross-border payment settles in seconds.

---

[52] Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2018* (May 2019), available at: https://www.federalreserve.gov/publications/2019-economic-well-being-of-us-households-in-2018-banking-and-credit.htm.

[53] *Supra* note 7.

[54] United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, Goal 10.c, available at: https://sdgs.un.org/sites/default/files/publications/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf.

[55] *Supra* note 8.

Self-hosted wallets play a critical role in allowing that new remittance flow: rather than relying on a string of intermediaries to facilitate a payment, a user can — after accessing the network through a regulated on/off ramp — hold their balance in their currency of choice, and transfer that value in a single transaction to remit funds back home, all without incurring high fees. As the Blockchain Association notes in their report on self-hosted wallets, "If migrants are able to send remittances using self-hosted wallets, the exorbitant fees charged by the intermediaries facilitating these transfers will be greatly reduced. More money will go to the people who actually need it, and thus greater financial inclusivity around the globe will be engendered through the implementation of peer-to-peer transactions using self-hosted wallets."[56]

One potential consequence of the NPRM is that BSA-regulated entities which, in the U.S., serve as the fiat on/off ramps to blockchain networks, may decide that transacting with self-hosted wallets is too risky or that they are viewed by regulators with disfavor. They may opt to "de-risk" their CVC business by refusing to interact with self-hosted wallets. In this case, they would be closing off access to blockchain-based financial services to millions of unbanked Americans. This would reserve the increased efficiencies and cost savings of blockchain technology to those already on the inside and further marginalize those who are not.

D. The NPRM will hinder U.S. global competitiveness, discourage domestic innovation and incentivize offshoring of a critical technology.

FinCEN acknowledges the "inherently international nature of CVC" in the NPRM.[57] However, it does not seem to appreciate what that means in terms of the United States' economic and national security competitiveness. In October 2020, the U.S. Government published its National Strategy for Critical and Emerging technologies (the "National Strategy").[58] Among the 20 critical and emerging technologies identified in the National Strategy are "distributed ledger technologies." In our view, that plainly encompasses both blockchain and self-hosted wallet technologies. The National Strategy is built on two "pillars of success," which it identifies as (1) "promote the national security innovation base" and (2) "protect technology advantage."[59] Among the goals that make up pillar one are the following:

- Develop the highest-quality science and technology (S&T) workforce in the world,
- Attract and retain inventors and innovators,
- Leverage private capital and expertise to build and innovate,
- Rapidly field inventions and innovations, and
- Reduce burdensome regulations, policies, and bureaucratic processes that inhibit innovation and industry growth.

The NPRM runs directly counter to the goals of the National Strategy. The NPRM is a burdensome regulation that would impose massive new bureaucratic processes on industry which will, in turn, inhibit innovation. Meanwhile, global adversaries such as the People's Republic of China are investing heavily in

[56] *Supra* note 4.
[57] NPRM at 83854.
[58] National Security Council, *National Strategy for Critical and Emerging Technologies* (October 2020), available at: https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.
[59] *Id*.

blockchain technologies.[60] Chinese President Xi Jinping famously vowed that China would "seize the opportunities" presented by blockchain technology.[61] China's Digital Currency Electronic Payment (DCEP)[62] and Blockchain Service Network (BSN) initiatives are the digital manifestation of their Belt and Road Initiative. And, while China pours resources into developing its blockchain industry, U.S. agencies, through measures such as the NPRM, take actions that will make the U.S. a less desirable jurisdiction for blockchain innovation and make the U.S. blockchain industry less competitive.

While the nature of blockchain technology is "inherently international," the jurisdictional reach of FinCEN is not. Given the cumulative (and growing) weight of blockchain regulations in the U.S.,[63] one possible result of that mismatch is that American blockchain entrepreneurs and innovators may choose to relocate existing businesses or start new businesses outside the U.S., and foreign innovators who might have otherwise chosen to launch or grow their businesses here may instead choose friendlier jurisdictions. This eventuality also runs counter to the National Strategy's goal of "attract[ing] and retain[ing] inventors and innovators." In fact, it is more likely to cause the flight of such talent.

There is a better way than the approach taken in the NPRM – one that would harmonize with the National Strategy. Instead of treating all self-hosted wallets as inherently suspicious, FinCEN could partner with U.S. based blockchain analytics firms to develop the tools and technologies to identify and trace truly suspicious blockchain activity without needlessly burdening the entire industry and intruding upon the private affairs of law-abiding Americans. Not only would such an approach be more effective and less burdensome, but it would also fulfill two more goals of the National Strategy, namely to "encourage public-private partnerships" and "develop and adopt advanced technology applications within government and improve the desirability of the government as a customer of the private sector."

V. New technology deserves new approaches to regulation.

The BSA was designed to regulate a centralized, intermediary-based financial system. Blockchain technology was conceived as a decentralized system intentionally independent of intermediaries. Therein lies the inherent friction of applying the BSA to a technology (self-hosted wallets, in this case) to which it fundamentally does not fit. Continuing down this road is likely to result in unintended consequences, several of which we outline above. For example, the technological differences between a bank account number and a blockchain address could have sweeping privacy and cybersecurity implications if BSA principles were rigidly applied to both. Foisting antiquated rules onto entirely new paradigms doesn't work - and it won't work here.

---

[60] *See, e.g.*, Werbach, Kevin, Wired, *Opinion: China is Pushing Toward Global Blockchain Dominance* (November 12, 2019), last accessed January 2, 2021 at: https://www.wired.com/story/opinion-china-is-pushing-toward-global-blockchain-dominance/.

[61] Kharpal, Arjun, CNBC, *With Xi's backing, China looks to become a world leader in blockchain as US policy is absent* (December 15, 2019), last accessed January 2, 2021 at: https://www.cnbc.com/2019/12/16/china-looks-to-become-blockchain-world-leader-with-xi-jinping-backing.html .

[62] Vincent, Danny, BBC News, *'One day everyone will use China's digital currency'* (September 24, 2020), last accessed January 2, 2021 at: https://www.bbc.com/news/business-54261382.

[63] While the NPRM would be just one of a number of potentially applicable regulations to U.S. blockchain-based businesses, EO 12866(1)(b)(11) requires agencies to consider "the costs of cumulative regulations."

Of course, we fully support FinCEN's mission. Preventing financial crime is good for blockchain just as it is good for society. SDF and the larger blockchain industry stand ready to work cooperatively with FinCEN to leverage the technological breakthroughs of blockchain in furtherance of this mission. Only by collaborating with the blockchain industry can FinCEN truly maximize the net benefits of its regulations in this cutting-edge field. Blockchain analytics, which leverages the transparency and immutability of the blockchain, as we mentioned throughout this letter, would be a great place to start.

We respectfully urge FinCEN to partner with the private sector to develop a tailored and technologically congruous approach to achieving its regulatory objectives while allowing the industry to deliver on this new technology's potential to solve old problems, such as empowering unbanked populations with new approaches to financial services.

* * * * *

SDF appreciates the opportunity to comment on the NPRM. We believe that there are better approaches, both substantively and procedurally, to rulemaking in this area and we strongly encourage FinCEN to put arbitrary deadlines aside and take the time necessary to achieve a thoughtful and balanced result. In addition to our direct comments presented in this letter, we note that the SDF is a member of both the Blockchain Association and the Chamber of Digital Commerce and we support, echo, and reiterate the comments and recommendations more fully set forth in their submissions to the NPRM.

Sincerely,

Denelle Dixon
Chief Executive Officer & Executive Director
Stellar Development Foundation

HELLOSIGN

Audit Trail

TITLE	NPRM Comment Letter
FILE NAME	Stellar Developme...ment.1.4.2021.pdf
DOCUMENT ID	63a6329ef42b3fe6dcaa2b4256e49477e06c12ae
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Completed

Document History

SENT	**01** / **04** / **2021** 17:08:58 UTC-8	Sent for signature to Denelle Dixon (denelle@stellar.org) from legal@stellar.org IP: 24.4.59.121
VIEWED	**01** / **04** / **2021** 17:13:19 UTC-8	Viewed by Denelle Dixon (denelle@stellar.org) IP: 24.130.250.3
SIGNED	**01** / **04** / **2021** 17:13:30 UTC-8	Signed by Denelle Dixon (denelle@stellar.org) IP: 24.130.250.3
COMPLETED	**01** / **04** / **2021** 17:13:30 UTC-8	The document has been completed.