ANDREESSEN HOROWITZ

January 4, 2021

BY U.S. MAIL AND ELECTRONIC SUBMISSION

Kenneth A. Blanco
Director, Financial Crimes Enforcement Network
FinCEN Policy Division
P.O. Box 39
Vienna, VA 22183

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

Dear Director Blanco,

Andreessen Horowitz ("a16z") has significant and direct interests in the proposed rulemaking and respectfully requests that the Financial Crimes Enforcement Network ("FinCEN") address the many serious legal and policy concerns identified here, and in comments by other stakeholders, before acting on a rule, the consequences of which FinCEN appears not to have fully considered in its rush to push it through.

INTRODUCTION AND EXECUTIVE SUMMARY

Late on the Friday before Christmas, with only a month before a new administration takes office, FinCEN announced a Notice of Proposed Rulemaking (the "NPRM")[1] that has the potential to negatively impact what the White House has labelled the "critical and emerging" virtual currency industry.[2] During the Christmas and New Year holiday season, FinCEN published a 22-page NPRM in the *Federal Register* on December 23, 2020, and gave the public until only January 4, 2021—*six* business days—to provide comments on what is, arguably, the most significant rulemaking to address the virtual currency industry that FinCEN (and perhaps any federal agency) has ever released. The rule would regulate self-hosted wallets, which are

[1] U.S. Dep't of the Treasury, Press Release, *The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions* (Dec. 18, 2020), https://home.treasury.gov/news/press-releases/sm1216; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840 (proposed Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022) (hereinafter "NPRM"), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf.

[2] White House, *National Strategy for Critical and Emerging Technologies* (Oct. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

software applications that store users' cryptographic keys and allow them to transact with assets on the blockchain directly, rather than through a financial institution. But the rule—which appears to have been hastily drafted in order to rush it through at the end of the administration—is both unlawful and ill-conceived as a policy matter.

Indeed, as described throughout these comments, the rulemaking is substantively and procedurally defective in critical respects. The Administrative Procedure Act ("APA")[3] mandates that federal agencies provide stakeholders and members of the public with a meaningful opportunity to comment on proposed regulations to ensure that regulations are well-reasoned and do not have unintended consequences. The gravity and uncertainty of the consequences likely to flow from this rule, if it were to be adopted, the brevity of the comment period, and FinCEN's failure to engage meaningfully with the regulated community in advance of the NPRM's publication mean that the proposed rule is the very definition of rulemaking that is arbitrary, capricious, and contrary to law.

a16z has direct and substantial interests in ensuring that federal regulators, like FinCEN, strike the appropriate balance with respect to the regulation of the nascent, fast-evolving virtual currency marketplace. a16z is one of Silicon Valley's leading venture capital firms. It has $16.5 billion under management and was an early investor in Facebook, Slack, Github, Okta, Pinterest, Lyft, Airbnb, Coinbase and dozens of other leading technology companies. In 2018, a16z established its first stand-alone fund focused on investing in the virtual currency ecosystem. Since then, it has launched a second virtual currency investment fund and has $865 million under management across both crypto funds. As an investor in numerous blockchain-based and virtual currency-related companies, a16z is well-positioned to evaluate the potential impact of the NPRM on the blockchain and virtual currency industry as a whole; and that impact is likely to be both substantial and wholly unjustified by the factual assertions FinCEN offers in the NPRM.

For the reasons set out in this letter, FinCEN should rescind the NPRM, or at a minimum, extend the comment period for at least 60 days, so that all stakeholders and the public can properly evaluate the rule's potential impact and provide meaningful feedback to FinCEN, as the APA requires. As we describe in more detail below, adopting the NPRM as a final (or interim final) rule would be arbitrary, capricious, and contrary to law for several independent reasons.

First, FinCEN offers no defensible reason for dispensing with traditional notice-and-comment rulemaking procedures in favor of a truncated six-business-day comment period over the holidays. FinCEN's failure to permit meaningful comment on the rule plainly violates the APA.

Second, the rule imposes a novel requirement—one found in no other Part of FinCEN's

[3] 5 U.S.C. § 551 *et seq.* (1946).

regulations implementing the Bank Secrecy Act ("BSA")—to collect and potentially verify identifying information not about customers, but about the *counterparties* of customers in all cases. The anemic factual record that FinCEN has assembled in no way justifies such a dramatic expansion of the BSA, which would impose, for the first time, a "Know Your Customer's Counterparty" requirement on banks and Money Services Businesses ("MSBs") that fall within the scope of the proposed rule (collectively, "Covered Entities"). This novel and sweeping information collection mandate also raises significant Fourth Amendment concerns.

Third, the rule unreasonably sweeps far broader than its purported justification. By its plain terms, the rule would capture Covered Entities' interactions with Decentralized Applications ("dApps"), and staking. There is no legal or policy rationale for this overbreadth.

Fourth, key components of the proposed rule fail to clearly convey to Covered Entities what they are expected to do. This lack of clarity will lead to inconsistent interpretations and implementation among state regulators—exactly the opposite of what FinCEN should want if the rule addresses "substantial national security concerns."[4]

Fifth, FinCEN failed to meaningfully account for, or seek to mitigate, the foreseeable negative effects of the proposed rule in ways that are likely to undermine its purported objectives of protecting national security and financial integrity.

For these reasons and others, FinCEN's proposed rule is arbitrary and capricious and is inconsistent with the APA. An agency may not adopt a regulation that is in violation of the law in such myriad ways and force the courts to step in to overturn it. It is the job of the executive branch and the agency to ascertain the legality of a regulation before promulgating it and even a cursory look at this NPRM fails under the most basic examination.

Important participants in the virtual currency industry, including responsible stakeholders like a16z, recognize the financial integrity risks in certain cryptocurrency activity, as in all financial activity, and eagerly seek a constructive dialogue with FinCEN about those risks. Although this comment letter represents an effort to identify several key shortcomings with the rule, the abbreviated comment period does not permit the opportunity to present meaningful feedback and analysis to the agency. Because receiving such feedback is the cornerstone of effective rulemaking and what the APA demands, FinCEN should rescind this proposed rule or, at least, extend the comment period for 60 days so that stakeholders can provide full and meaningful reactions with an eye toward improving it and accomplishing shared goals in a spirit of collaboration. The stakes are high in regulating a fast-evolving industry like cryptocurrency, and faithful adherence to sound regulatory decision-making principles is especially important in this context to avoid throttling innovation or generating unintended consequences.

[4] NPRM at 83842.

DISCUSSION

I. FINCEN HAS NOT DEMONSTRATED A NEED TO DISPENSE WITH NORMAL NOTICE AND COMMENT PROCESSES

The rulemaking is procedurally defective from the outset: FinCEN's decision to provide only *six* business days after publication of the NPRM in the *Federal Register* for the industry and the public to comment during the Christmas and New Year's holidays violates the APA and is itself cause to withdraw the rule or to at least extend the comment period. As FinCEN recognizes in the NPRM, the APA "generally requires" that "agencies must provide the public with a 'meaningful opportunity' to comment" on proposed rules.[5] The window is usually at least 30 days, and indeed, *FinCEN has provided at least that long for every substantive rulemaking of which we are aware it has conducted in the past 20 years*. While shorter periods may be appropriate in limited instances, these instances "are generally characterized by the presence of exigent circumstances in which agency action was required in a mere matter of days," such as a national emergency or a statutory deadline.[6] No such circumstances exist here.

FinCEN claims three justifications for its truncated comment period: (1) that "significant national security imperatives … necessitate an efficient process" for rulemaking; (2) that FinCEN has engaged with the cryptocurrency industry on AML risks in the virtual currency space; and (3) that the "foreign affairs" or "good cause" exceptions exempt this rulemaking entirely from notice-and-comment requirements. None of these justifications supports limiting the comment period here.

FinCEN does not assert that it has newly learned of emergent circumstances requiring immediate rulemaking; indeed, its self-professed engagement with the cryptocurrency industry over the past eighteen months suggests that the agency has long been aware of the issues addressed by this NPRM.[7] And the foreign affairs and good cause exceptions FinCEN half-heartedly invokes are intended for situations in which providing notice and an opportunity to comment would *itself* be detrimental.[8] FinCEN cannot plausibly claim that allowing public comment would be detrimental *while also* providing the opportunity to provide comment.

---

[5] *Id.* at 83852.

[6] *N. Carolina Growers' Ass'n, Inc. v. United Farm Workers*, 702 F.3d 755, 770 (4th Cir. 2012).

[7] FinCEN asserted that it "has engaged with the cryptocurrency industry on multiple occasions on the AML risks presented in the cryptocurrency space and carefully considered information and feedback received from industry participants." NPRM at 83841.

[8] *See* 5 U.S.C. § 553(b) (good cause exception applies when notice and comment are "impracticable, unnecessary, or contrary to the public interest"); *East Bay Sanctuary Covenant v. Trump*, 950 F.3d 1242, 1279 (9th Cir. 2020) (foreign affairs exception applies only if "the public rulemaking provisions should provoke definitely undesirable international consequences").

Having decided to engage in notice-and-comment rulemaking, FinCEN must give interested parties a meaningful opportunity to participate. It has not done so, and any rule emerging from this unreasonably truncated process will not survive legal challenge on this basis alone. Moreover, the substantive flaws in the proposed rule identified below underscore the importance of meaningful, not perfunctory, engagement with stakeholders in this context. In no interaction with a16z, or of which a16z is aware, did FinCEN share details of the substance of the proposed rule. Even letters that were sent by industry participants were written on the basis of mere rumors about the rule FinCEN was contemplating. These kinds of abstract discussions fail to justify the truncated comment period; in any event, informal consultations with industry cannot supplant the requirements of the APA.

II. FinCEN's Description of the Risk Does not Justify an Unprecedented Expansion of the BSA

The NPRM proposes something both unprecedented and unwarranted; without identifying evidence or tailoring the rule to mitigate specific risks related to the use of self-hosted wallets, FinCEN's purported objective,[9] FinCEN proposes to extend by regulation an obligation on Covered Entities to collect and potentially verify identifying information on *counterparties* of their customers *in all cases*. FinCEN has failed to articulate the policy rationale for imposing such novel compliance obligations.

A. *The Proposed Rule Would Impose Unprecedented Information Collection Obligations*

FinCEN's regulations implementing the BSA do not, in any other context, impose an obligation on financial institutions to know and potentially verify their customers' counterparty's identifying information in all cases—and FinCEN has provided no reliable evidence of any extreme risks involved in crypto transitions with self-hosted wallets to justify the imposition of this unprecedented obligation. The relevant portions of the proposed rule require Covered Entities to collect certain identifying information on the counterparty of their customer, specifically name and address, and "such other information as the Secretary may require."[10] The trigger for this information collection requirement is a "deposit, withdrawal, exchange, or other payment or transfer, by, through, or to" a Covered Entity that "involves a transaction in convertible virtual currency or a digital asset with legal tender status."[11] Transactions greater than $3,00 trigger a recordkeeping requirement while transactions greater than $10,000 require a

---

[9] U.S. Dep't of the Treasury, Press Release, *The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions* (Dec. 18, 2020), https://home.treasury.gov/news/press-releases/sm1216.

[10] NPRM at 83860.

[11] *Id.*

report to FinCEN.

The NPRM suggests that its requirements are similar to those imposed by the existing Currency Transaction Reporting ("CTR") requirement.[12] But that is incorrect. Because the proposed rule's reporting and recordkeeping requirements mandate collection of information about the counterparties of customers for transactions conducted entirely online, the rule's reach would go beyond the existing CTR Requirement,[13] which applies when people physically present themselves to a financial institution and conduct certain transactions in coins and paper money. The CTR regulations also do not require collection of information regarding the purpose of the cash transaction or any recipient of cash that is withdrawn beyond the person who is himself or herself withdrawing it. It also goes beyond the requirements of the Recordkeeping and Travel Rules, which require retention and transmission of identifying information about a counterparty if that information is included in the relevant payment or transmittal order;[14] the Recordkeeping and Travel Rules are not a similar mandate to *collect* and potentially verify identifying information about counterparties *in all cases*.

FinCEN has pledged to follow a "technology neutral approach" to regulation pursuant to the BSA in which the financial integrity risks, rather than the technology at issue, dictate the specific requirements to which financial institutions are subject.[15] The proposed rule breaks sharply with that commitment by imposing an entirely novel regulation *on a specific technological means of conducting transactions*—self-hosted wallets—that is unmoored from the risks that FinCEN has described. A core component of the BSA is that a financial institution must Know its Customer. This requirement is intentionally broad: financial institutions must tailor their AML compliance programs to the risks presented to their specific institution. Given that those risks may vary significantly, regulatory expectations about the compliance programs intended to mitigate those risks also vary. But, as far as we are aware, in no situation do

---

[12] *Id.* at 83844 ("[t]he reporting requirements of this proposed rule are a virtual currency analogue to the CTR reporting requirement.").

[13] While the Currency Transaction Report regulations require banks and MSBs to "verify and record the name and address of the individual presenting a transaction[,]" those rules apply when someone physically appears at a financial institution and attempts to engage in certain transactions with coin or paper money. *See* 31 C.F.R. § 1010.312; 31 C.F.R. § 1020.312; 31 C.F.R. § 1022.312.

[14] The Recordkeeping Rule for banks and non-bank financial institutions requires them to collect and retain the name and address of the beneficiary of a transaction if "received with the payment order," for banks (31 C.F.R. § 1020.410(a)(1)(i)(F)(1)), and if "received with the transmittal order," for nonbank financial institutions (31 C.F.R. § 1010.410(e)(1)(i)(F)). The Travel Rule only requires transmission of the name and address of the recipient of the transaction if "received with the transmittal order," not in all cases. 31 C.F.R. § 1010.410(f)(1)(vi).

[15] Kenneth A. Blanco, Director, FinCEN, Prepared Remarks delivered at the Consensus Blockchain Conference (May 13, 2020), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain; Kenneth A. Blanco, Director, FinCEN, Prepared Remarks at Chainalysis Blockchain Symposium (Nov. 15, 2019), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-chainalysis-blockchain-symposium.

FinCEN's regulations implementing the BSA command a financial institution to know the customers of its customers in *all* circumstances with respect to an entire category of transactions; the NPRM would tread new ground.

The closest comparison to this obligation arises in the correspondent banking context.[16] There, the BSA requires banks broadly to understand the correspondent banking customer's *customer base*, but only seldom might a financial institution subject to the BSA know and collect information about the identities of specific customers of its respondents. Here, the proposed rule requires that Covered Entities collect information on their customers' counterparties, and potentially take steps to verify such information, *in all cases*. This goes well beyond the requirements applicable to correspondent bank transactions and is not appropriately tailored to the risk FinCEN has described.

B. *FinCEN Does Not Justify the Departure from Past Practice with Evidence*

One would expect that the unprecedented nature of the proposed rule would be justified by a rigorous presentation of data related to the (commensurately extreme) illicit finance risks posed by transactions with self-hosted wallets, but it is not. FinCEN's failure in this regard is three-fold: (1) it presents only anecdotes, rather than comprehensive data, on the risks posed specifically by self-hosted wallets; (2) it neglects to impose specific regulatory requirements on some types of cryptocurrency activity despite recognizing that such activity poses the same types of risks related to anonymity as self-hosted wallets; and (3) it does not put in context the illicit finance risks posed by cryptocurrency in light of the relatively limited size of the cryptocurrency ecosystem when compared to fiat currency transactions. As such, the NPRM fails the most basic requirement of the APA that rulemaking consider all relevant factors and analyze important aspects of the issue identified by the agency.[17] If given more time during the comment period, stakeholders and the public could be able to provide data and detailed studies about transactions conducted with self-hosted wallets or suspected illicit activity involved in virtual currency transactions, but the abbreviated comment period FinCEN elected makes doing so impossible.

1. <u>FinCEN Presents Only Anecdotes about Illicit Use of Self-Hosted Wallets</u>

First, a significant amount of the information FinCEN presents in the NPRM to describe the risks involved with self-hosted wallets pertains to cryptocurrency *generally*, rather than the use of self-hosted wallets specifically. FinCEN cites, for example, a single report by Chainalysis to note that "approximately 1% of overall market transaction volume, or $10 billion, in CVC

[16] In this context, banks are required to, *inter alia,* assess the money laundering risk posed by a correspondent account, including the "nature of the foreign financial institution's business and the markets it serves." *See generally* 31 C.F.R. § 1010.610; 31 C.F.R. § 1010.610(a)(2)(i).

[17] *See Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983).

activity conducted globally in 2019 was illicit."[18] FinCEN notes that its own data reveals "approximately $119 billion in suspicious activity reporting associated with CVC"[19] and that "malign actors have used CVC" to facilitate activities that threaten the United States, including weapons proliferation, transnational money laundering, and ransomware attacks.[20] But *how* FinCEN's SAR reports are "associated with CVC activity," let alone with self-hosted wallets, the problem the NPRM purports to address, is left unsaid. To justify the significant negative impact that would be caused by the proposed rule, FinCEN should demonstrate the scale of the threat posed by Covered Entities' interactions with self-hosted wallets, and then show how its proposed rule would deter or prevent that activity.[21] FinCEN, in its rush to propose this rule before the end of the administration, has not done so. With more time, FinCEN and the industry could engage in more robust analysis of risks attendant with the use of self-hosted wallets.

2. FinCEN Describes High-Risk Cryptocurrencies It Does Not Subject to Specific Regulation Despite Shared Concerns Related to Anonymity

Second, and further illustrating the tenuous relationship between the problem FinCEN purports to identify and the rule it has drafted, the agency cites illicit finance risks attendant with other forms of cryptocurrency, such as Anonymity Enhanced Cryptocurrencies ("AECs"), whose transactions are generally not traceable on public blockchains. If anonymity is FinCEN's true animating concern with respect to self-hosted wallets, the focus of its regulatory energy should be on those AECs whose blockchains do not allow the tracing of transactions. FinCEN fails, however, to either subject transactions in AECs to specific regulation, or to explain why it is not doing so. This disconnect between the rule FinCEN proposed and the purported risks it has identified cannot be justified, and makes the rule vulnerable to legal challenge on this additional basis.

[18] NPRM at 83842.

[19] *Id.*

[20] *Id.* at 83842-43 (Emphasis added).

[21] In moving forward with rulemaking focused on self-hosted wallets, FinCEN cites an anecdote about the use of self-hosted wallets in financial crime, noting in a footnote to its NPRM that "across 2017 and 2018, FinCEN observed at least seventeen separate transactions over $10,000 conducted between U.S. financial institutions and unhosted wallets affiliated with the Lazarus Group, a malign actor engaged in efforts to steal and extort CVC as a means of generating and laundering large amounts of revenue for the North Korean regime." NPRM at 83843, fn.18. But these anecdotes do not amount to systematic analysis about the scale of the threat posed by self-hosted wallets or justify the scope of the proposed rule.

3. FinCEN Fails to Contextualize the Risk Related to Cryptocurrency in Light of the Overall Illicit Finance Risk in the U.S.

Finally, FinCEN cites limited public information, such as the *2020 Crypto Crime Report* by Chainalysis,[22] describing the risks attendant with cryptocurrency transactions, but it does not place those risks in context of the broader financial system. As a result, in violation of the APA's demand of reasoned decisionmaking, it magnifies the risks associated with cryptocurrency out of proportion to the volume of cryptocurrency transactions in the economy and it imposes a novel form of BSA regulation on activity that represents a negligible slice of overall transactional activity in the U.S. financial system.[23] For example, the *2018 National Money Laundering Risk Assessment* contains only a short section discussing the risks posed by virtual currency, alongside those posed by misuse of legal entities, bulk cash smuggling, and the use of complicit intermediaries like merchants and professionals, who are generally not subject to the BSA, to engage in money laundering.[24] As such, FinCEN is not behaving in a "technologically neutral" manner, where BSA rules are tailored to the scale of the illicit finance risks presented.

The scale of dollar clearing and cash transactions dwarf transactions involving cryptocurrency, let alone those involving self-hosted wallets, as do the Treasury Department's own estimates about the size of illicit activity in the traditional economy when compared with estimates about the amount of illicit activity involving cryptocurrency. The Clearing House Interbank Payments System alone, for example, clears and settles $1.5 trillion in domestic and international payments *each day*.[25] The NPRM implies the total annual volume of cryptocurrency transactions is $1 trillion, which is less than the currency transferred through the U.S. banking system in a single day,[26] while the market capitalization of *all* virtual currencies is approximately $850 billion as of the date of this letter.[27]

---

[22] *Id.* at 83842.

[23] The recently published *2020 National Strategy for Combating Terrorist and Other Illicit Financing*, which identifies the greatest risk posed to the U.S. financial system, identifies the risks posed by virtual currency use alongside these posed by correspondent banking and the use of cash," https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf ("[t]he significant volume of foreign funds and number of transactions that are intermediated through U.S. correspondent banks" and "[t]he ubiquitous and anonymous use of U.S. currency domestically and internationally.").

[24] *2018 National Money Laundering Risk Assessment,* at 4 (hereinafter "2018 NMLRA") https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

[25] The ClearingHouse, *CHIPS – About CHIPS*, https://www.theclearinghouse.org/payment-systems/chips.

[26] *See* NPRM 83840, 83842 (stating that an "industry estimate is that approximately 1% of overall market transaction volume, or $10 billion, in CVC activity conducted globally in 2019 was illicit." $10 billion is 1% of $1 trillion.).

[27] *Today's Cryptocurrency Prices by Market Cap*, https://coinmarketcap.com/ (last visited January 1, 2021).

And the 2018 National Money Laundering Risk Assessment estimates that financial crime *in the United States* generates $300 billion of proceeds for potential laundering, of which $100 billion is related to healthcare fraud. If the estimate FinCEN cites in its NPRM is correct and there is $10 billion per year of illicit cryptocurrency transactions *globally,* it is difficult to understand why novel AML requirements are being applied to Covered Entities instead of hospitals and health insurance companies, which experience an order of magnitude more financial crime each year *in the United States*.[28]

FinCEN nowhere explains why imposing regulations on this particular corner of the cryptocurrency market will have a material impact on the money laundering threat in the U.S., or why it represents a risk-based application of the BSA. If FinCEN had provided more time for comment, the public could have been able to present analyses on the risks posed by crypto transactions, including through self-hosted wallets, compared with other transaction types.

C. *FinCEN's Novel Approach Raises Significant Fourth Amendment Concerns*

The proposed rule's requirement to collect information from counterparties of customers also raises significant questions under the Fourth Amendment because it departs sharply from the information-gathering and reporting requirements that the Supreme Court has upheld. Banks are, of course, required to keep various information about their *customers*, and then turn the information over to the government when subpoenaed, or pursuant to a reporting requirement. But the precedents upholding these requirements rest on the theory that "[a]ll of the documents obtained . . . contain only information *voluntarily conveyed* to the banks and exposed to their employees in the ordinary course of business."[29] The proposed rule, on the other hand, would *mandate* that cryptocurrency exchanges collect information about their customers' counterparty in all cases. This requirement goes well beyond the framework the Supreme Court has approved in the context of records voluntarily handed over to a regulated entity in exchange for the provision of a service. It is not a voluntary assumption of risk; it is governmentally imposed coercion, forcing the exchanges, their customers, or their counterparties to collect or convey information they would not otherwise collect or convey in the ordinary course of business—solely to fulfill the government mandate.

The Supreme Court's recent cell phone location monitoring decision, *Carpenter v. United States*, makes clear that the precedents about "voluntarily conveyed" information do not apply when such voluntariness is absent.[30] The government could not engage in warrantless, probable-cause-less gathering of cell phone location information, the Court held, because a "rationale underlying the third-party doctrine—voluntary exposure—[does not] hold up when it comes to"

---

[28] 2018 NMLRA at 2.

[29] *United States v. Miller*, 425 U.S. 435, 442 (1976) (emphasis added).

[30] 138 S. Ct. 2206 (2018).

such information.[31] "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[32] Likewise under the proposed rule, the turning over of counterparty information would be compulsory, not voluntary, with the only option being the customers' "disconnecting [themselves] from the [virtual currency] network."

The cases upholding the BSA against constitutional challenge also stressed that the information banks were required to keep and disclose was information that "[m]any banks [had] traditionally kept."[33] "By requiring that such records be kept by all banks, the Bank Secrecy Act is not a novel means designed to circumvent established Fourth Amendment rights."[34] But no such custom exists for identifying information about *counterparties* of customers; while banks are required to report certain cash withdrawals, they do not generally require the customers to explain what they will be doing with the cash or to whom they will give it. The kind of information-gathering contemplated by the proposed rule is thus indeed "a novel means" for defeating the privacy of bank customers and the third parties with whom they seek to deal.

III. THE PROPOSED RULE IS OVERLY BROAD, SWEEPING UP SIGNIFICANT ACTIVITY THAT DOES NOT INVOLVE SELF-HOSTED WALLETS

FinCEN's purported motivation for publishing the NPRM is "the illicit finance threat created by <u>one</u> segment of the CVC market"[35]—self-hosted wallets. But the rule as drafted sweeps in substantial additional conduct about which FinCEN has failed to identify *any* illicit finance risk or justification for rulemaking, suggesting that the agency again violated a core tenet of the APA by failing to consider important aspects of the issue under consideration.[36]

Specifically, the proposed rule purports to force Covered Entities to collect personally identifiable information when their customers engage in staking transactions and when they contribute assets to certain dApps.[37] dApps are software programs that run on blockchains,

---

[31] *Id.* at 2220.

[32] *Id.*

[33] *Miller*, 425 U.S. at 444.

[34] *Id.*

[35] NPRM at 83841 (emphasis added).

[36] *See State Farm*, 463 U.S. at 42.

[37] Most dApps today run on the Ethereum blockchain network and are applications for which the distributed nature of the network facilitates the underlying activity more efficiently or effectively than existing platforms. dApps can perform a variety of functions, for example, facilitating digital storage and retrieval of data (through a dApp called "Filecoin"), creating new ways of paying for Internet advertising (through the Basic Attention Token and Brave Browser), and matching borrowers and lenders of virtual currency (through the Aave dApp).

while "staking" is a way for holders of virtual currencies to participate in the validation of transactions on blockchain networks and earn rewards for doing so. When customers engage in these activities through a Covered Entity, the proposed rule would likely cover these activities because they would be transfers "by" a Covered Entity that "*involve[]* a transaction in convertible virtual currency."[38] But in both staking and dApp transactions, Covered Entities would transmit assets to a blockchain address or smart contract, with respect to which there is no identifiable "counterparty" about whom a Covered Entity can collect "the name and address."[39] As a result of this overbreadth, Covered Entities could be prevented from engaging in these perfectly legitimate commercial activities as to which FinCEN has alleged *no* illicit finance risks.

FinCEN should therefore, at a minimum, clarify that the rule does not apply to these types of transactions. If the public had additional time to develop comments, it could potentially identify additional examples of the rule's overbreadth, and provide assessments of the economic impact of FinCEN's proposed rule. Specifically, it may be possible to provide detailed studies on the use of dApps over time, their evolving business models, how Covered Entities could play a role in the dApp ecosystem, and how this rule could affect Covered Entities' participation in these activities. The response thus has been constrained by the extremely short comment period.

IV. KEY COMPONENTS OF THE PROPOSED RULE ARE SO VAGUE THEY CANNOT BE IMPLEMENTED EFFECTIVELY OR UNIFORMLY

In addition to the rule's overbreadth, key obligations imposed by the proposed rule are so ill-defined and ambiguous that they will likely be interpreted differently not only by Covered Entities, but also by the state regulators that license and examine them. Implementation of the rule will therefore likely be inconsistent, which will undermine the national security objectives the proposed rule is meant to accomplish and present a significant litigation risk for FinCEN.[40]

A. *The Rule is Ambiguous about Whether Covered Entities Must Verify Information about Counterparties of their Customers*

The proposed rule is especially ambiguous about what additional information must be collected of counterparties beyond name and address. This is true in two principal ways. First, by leaving open the possibility that the Secretary may mandate the collection of "other

---

[38] NPRM at 83860.

[39] *Id.*

[40] It is "[a] fundamental principle in our legal system ... that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations*, 567 U.S. 239, 253 (2012). Accordingly, it follows that "[a]n agency cannot enforce a rule against a party if it is unduly vague or if the party did not otherwise have fair notice of the rule." *TNA Merch. Projects, Inc. v. Fed. Energy Regulatory Comm'n*, 857 F.3d 354, 360 (D.C. Cir. 2017).

information,"[41] FinCEN introduces uncertainty into the compliance mandates of Covered Entities. Second, FinCEN introduces the possibility that Covered Entities will be required, by virtue of their risk-based AML programs, to "confirm the accuracy of counterparty information."[42] Both of these contingent obligations leave open the possibility that Covered Entities will need to collect information beyond names and physical addresses of the counterparties, and potentially to verify it.[43] But FinCEN does not clarify how it expects Covered Entities to "confirm the accuracy of counterparty information" given that they will not have direct relationships with the counterparties. This lack of clarity is about requirements fundamental to the rule's operation.

This ambiguity is exacerbated by the structure of financial regulation in the United States, which divides responsibility between state and federal regulators, and so virtually guarantees that the rule will be interpreted in different ways around the country. Other regulations related to banks' customer information program obligations avoid this problem by specifically enumerating the information that needs to be collected from customers at the point of onboarding.[44] The proposed rule, by contrast, leaves the specific information that needs to be collected to be interpreted differently by the state regulators who license and supervise banks and MSBs.

B. *The Rule Lacks Clarity on how Transactions May Qualify for the "Financial Institution" Exemption*

A second significant area of ambiguity in the proposed rule is how Covered Entities are supposed to determine whether transactions qualify for the exemption from recordkeeping and reporting requirements because they are with counterparties with "account[s] … held at a financial institution regulated under the BSA" or at certain foreign financial institutions.[45] Unlike in the context of fiat currency transfers, there is no standardized messaging scheme in the virtual currency context like the SWIFT system that conveys the name of the beneficiary financial institution and other information with every transaction between banks.[46] Thus, it is not clear how Covered Entities are meant to confirm that transactions are with other financial institutions.

---

[41] NPRM at 83850, 83860.

[42] *Id.* at 83849.

[43] *Id.* at 83859.

[44] 31 C.F.R. § 1020.220.

[45] NPRM at 83860.

[46] There is no way to tell on the face of a wallet address whether it is a self-hosted wallet, and thus subject to the recordkeeping and reporting requirements set out in the NPRM, or is instead associated with a financial institution in a specific jurisdiction, and thus exempt from them. While blockchain forensics tools can link certain blockchain addresses to particular financial institutions that use them, those tools do not have universal coverage.

Additional guidance in the NPRM on the exemption covering transactions with foreign financial institutions may further reduce its practical utility. To avail themselves of the exemption, Covered Entities must "apply reasonable, risk-based, documented procedures to confirm that the foreign financial institution *is complying* with registration or similar requirements that apply to financial institutions in the foreign jurisdiction."[47] Such a requirement could be read to demand not only that the Covered Entity have some knowledge of relevant local law to determine whether the foreign financial institution is appropriately registered, but also that it have some way of assessing whether a financial institution with which it has no formal relationship is, *at the time of the transaction*, complying with that law. How Covered Entities are supposed to make these determinations remains a mystery. But the practical impact of these measures is likely to be a dramatic reduction in transactions with wallet addresses that *may be* associated with foreign financial institutions, even for those transactions that FinCEN apparently has no concern with Covered Entities facilitating.

V. FINCEN FAILED TO MEANINGFULLY ACCOUNT FOR FORESEEABLE NEGATIVE EFFECTS OF THE RULE

In addition to the significant defects above, FinCEN has also failed to consider or account for the foreseeable negative effects of the rule. These failures disregard an agency's basic obligation under the APA to assess the benefits, as well as the drawbacks, of a proposed rule. [48] These effects are likely to materialize because Covered Entities are likely to react to the proposed rule's vagueness and overbreadth by simply prohibiting transactions with self-hosted wallets. Even if they do not do so, many customers of Covered Entities are likely to flee U.S.-based exchanges in reaction to the proposed rule.

The foreseeable effects of the proposed rule presented below represent a preliminary effort to describe the likely consequences of FinCEN's action. If FinCEN had not adopted such an abbreviated period for comment, it would have been possible for a16z and others to provide more detailed data and analysis on these effects. For example, a16z likely could have included more comprehensive statistics on the proportion of activity taking place on Covered Entities that would be impacted by the rule, and attempted to model how the rule would affect customer behavior. The abbreviated comment period effectively precluded this kind of analysis.

A. *Potential Harm to Law Enforcement Investigations*

Because the proposed rule will likely cause customers of Covered Entities to leave those

---

[47] NPRM at 83849 (emphasis added).

[48] FinCEN's failure to grapple with these predictable consequences will render the rule arbitrary and capricious because these consequences are certainly "an important aspect of the problem," *State Farm*, 463 U.S. at 43, and, as the Supreme Court has explained, "reasonable regulation ordinarily requires paying attention to the advantages *and* the disadvantages of agency decisions," *Michigan v. EPA*, 576 U.S. 743, 753 (2015).

exchanges in favor of offshore or unregistered exchanges, it will likely decrease the amount of information available to law enforcement that can be obtained from them through various types of legal process. The United States has a reasonably clear structure for regulating cryptocurrency exchanges, which has led to a generally productive relationship between those exchanges and law enforcement agencies. In fact, significant law enforcement successes involving cryptocurrency investigations have depended on productive partnerships between exchanges and the government.[49]

Exchanges are able to assist law enforcement investigations because they currently are repositories of information about the transactional activities that take place on their platforms. Through proper legal processes, law enforcement agencies are able to request information about transactional and customer information. In the summer of 2020, for example, the Twitter accounts of prominent figures such as President-elect Joseph Biden, former President Barack Obama, and Tesla CEO Elon Musk, were hacked. The scammers requested the accounts' followers to send cryptoassets to a specific wallet address; investigators used blockchain analytics to identify exchanges where the addresses were housed. The exchanges, in turn, provided identifying information about the individuals who opened the accounts.[50] If transactions move out of U.S. exchanges as a result of the rule, this type of information flow to law enforcement will decrease. Exchanges will also have a more difficult time with their own risk management if self-hosted activity moves away from them, though it is impossible to determine by *how much* in the abbreviated time for comment FinCEN provided. With additional time, a16z or others could potentially compile more systematic data on the likely impact the rule will have on Covered Entities' customers.

There is an additional challenge that is likely to materialize as a result of the proposed rule—it will make the forfeiture of cryptocurrency assets traceable to crime more difficult if they are not held on exchanges subject to U.S. jurisdiction. This will substantially impede a significant tool that law enforcement has deployed in the virtual currency space and which recently yielded the forfeiture of bitcoin worth over $1 billion derived from the Silk Road

---

[49] Usually, this involves law enforcement using blockchain forensic tools to identify cryptocurrency exchanges involved in transactions related to illicit activity, which then allows enforcement agencies to request additional specific information from the exchanges through subpoenas or other forms of legal process. For example, exchanges provided information to IRS-CI during the takedown of Welcome to Video, the largest child pornography repository. *See* U.S. Dep't of Justice, Press Release No. 19-1104, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin* (Oct. 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child; Complaint, *United States v. Twenty-Four Cryptocurrency Accounts*, No. 19-cv-3098 (D.D.C. filed Oct. 16, 2019) (ECF No. 1).

[50] Chainalysis Blog, *How Law Enforcement Used Blockchain Analysis to Follow Funds and Identify the Twitter Hackers* (July 31, 2020), https://blog.chainalysis.com/reports/chainalysis-doj-twitter-hack-2020.

criminal marketplace.[51] The NPRM completely ignores the negative impact of the proposed rule on law enforcement and asset forfeiture.

B. *Damaging Effects on Innovation in Blockchain Technology*

Another foreseeable consequence of the proposed rule that FinCEN failed to address is its likely adverse impact on innovation. Self-hosted wallets are foundational to the development of novel blockchain-based programs, including those that can operate in an autonomous fashion. Virtual currency miners, node operators, and developers all depend on interactions with self-hosted wallets to operate their systems. Those participants in the cryptocurrency ecosystem interact with Covered Entities in two principal ways. First, as described above, Covered Entities can facilitate interactions with these participants directly. And second, applications that interact directly only with self-hosted wallets rely on exchanges to facilitate the ability of users to purchase the tokens they need through those exchanges.

The scale of innovation taking place in this space is staggering—in 2020 alone, for example, the amount of value deployed in decentralized finance applications went from approximately $670 million to $14.2 *billion*, while the number of users increased tenfold, from approximately 100,000 to 1.2 million.[52] If FinCEN restricts the accessibility of self-hosted wallets, blockchain application developers will likely focus their energies on jurisdictions outside the United States where it will be easier for them to develop a robust ecosystem around their applications, allowing other countries to reap the benefits derived from serving as a home for the next generation of companies. The White House itself recognized the importance of blockchain by identifying distributed ledger technology as a "critical and emerging technology," in which it wants the United States to "maintain worldwide leadership."[53] But FinCEN does not explain how its rule is consistent with this goal. FinCEN should specifically consider this question before it promulgates a final rule given the likely impact on blockchain software developers. And had it had more time, a16z would have been able to provide additional information about it.

C. *Exclusion of Financially Vulnerable Population*

FinCEN also fails to evaluate the impact the proposed rule is likely to have on financially vulnerable segments of the population both within and outside the United States. The World Bank Group estimates that about 2 billion adults are excluded from the financial system and Yale University estimates about 2 percent of the world's population may be homeless, with another

---

[51] *See, e.g.*, U.S. Dep't of Justice, Press Release, *United States Filed a Civil Action to Forfeit Cryptocurrency Valued at Over One Billion U.S. Dollars* (Nov. 5, 2020), https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us.

[52] *See* https://defipulse.com/; https://explore.duneanalytics.com/dashboard/defi-users-over-time.

[53] White House, *National Strategy for Critical and Emerging Technologies* (Oct. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

20% lacking adequate housing. [54] Because of the increasing number of people who have access to smartphones,[55] these individuals, who are disproportionately poor and female, are more likely to use self-hosted wallets to receive remittances or engage in other transactions, just as poor or undocumented workers are more likely to transfer money through non-bank financial institutions like money transmitters or with money orders. This is because using banks or MSBs may be too expensive or too distant, because they may not trust those institutions or may not use them because local currencies are experiencing hyperinflation, or because they may not have stable physical addresses to obtain identity documents.[56]

D. *Harmful Effects to Privacy and Human Rights*

FinCEN's proposed rule also threatens to have significant negative implications for privacy and human rights. While certain regulations may be necessary to ensure the prevention of illicit activities, the recordkeeping and reporting requirements here intrude on individuals' privacy interests without well-founded reasons. The proposed rule requires that customers of Covered Entities report the names, physical addresses, and potentially other sensitive information about their counterparties, potentially without the knowledge or consent of the counterparties themselves. Given that Non-Governmental Organizations will likely have the greatest insights into the impact of the proposed rule on human rights interests—for example, entities such as Kiva or Mercy Corps (both of whom have devoted considerable resources to crypto given the inclusion it can bring)—but have the least resources to submit detailed comments in this compressed time period, FinCEN is depriving itself of valuable perspectives on a critically important dimension of the problem by not extending the comment period; it is also violating the APA by failing to provide interested parties a meaningful opportunity to provide their input.[57]

---

[54] Asli Demirguc-Kunt et al., *Bringing the 2 Billion Unbanked into the Financial System*, World Bank Group (Apr. 2015), https://www.worldbank.org/content/dam/Worldbank/Research/GlobalFindex/PDF/N2Unbanked.pdf; Joseph Charmie, YaleGlobal Online, *As Cities Grow, So Do the Numbers of Homeless* (July 13, 2017), https://yaleglobal.yale.edu/content/cities-grow-so-do-numbers-homeless.

[55] A 2018 study found that approximately one-third of the homeless population over 50 years old had access to a smartphone, and thus, potentially, to the ability to engage in virtual currency transactions with self-hosted wallets. Raven, Maria C., et. al., *Mobile Phone, Computer, and Internet Use Among Older Homeless Adults: Results from the HOPE HOME Cohort Study*, JMIR MHealth and UHealth e10049 (Dec. 2018), https://mhealth.jmir.org/2018/12/e10049/.

[56] The Global Findex survey found that in "the Middle East, 41 percent of adults without an account say they cannot get one. This likely reflects prohibitive costs and documentation requirements for opening an account." Demurguc-Kunt et al., *supra* note 54.

[57] *See, e.g.*, *Prometheus Radio Project v. FCC*, 652 F.3d 431, 450 (3d Cir. 2011) ("meaningful opportunity … means enough time with enough information to comment and for the agency to consider and respond to the comments").

E. *Lack of Time to Provide Detailed Analysis on Impacts of Proposed Rule*

FinCEN requests additional information about quantitative data for complying with the requirements of the rule, but many of the specific questions for comment request information about quantification of the costs and benefits that cannot be reasonably or properly analyzed in a comment period encompassing six business days. Indeed, FinCEN seeks comment on two dozen specific questions, in addition to the more general questions about the feasibility of implementing the rule, and the other issues we have addressed in this letter.[58] We agree that the questions FinCEN asks are important and the fact that FinCEN has asked them only underscores the need for FinCEN to further analyze these issues after providing stakeholders a genuine time to collect relevant information that should inform FinCEN's actions in this space.

VI. COURTS WILL HOLD THAT THE UNDERLYING RULE IS ARBITRARY AND CAPRICIOUS

For all of the reasons cited above, FinCEN's Proposed Rule is arbitrary and capricious in its current form, violating numerous basic requirements of reasoned decision-making—including that an agency "examine the relevant data and articulate a satisfactory explanation for its action including a 'rational connection between the facts found and the choices made'"[59]; that the agency not irrationally ignore the disadvantages of a proposed regulation;[60] and that the agency genuinely consider evidence contradicting its position.[61]

Beyond these defects, FinCEN's Proposed Rule also fails the requirements of reasoned decisionmaking in at least two additional respects.

First, the Proposed Rule is arbitrary and capricious because it fails to provide a phase-in period during which cryptocurrency exchanges can implement measures to comply with the new rule, which could—and likely would, given the brevity of the comment period and the upcoming inauguration—go into effect this month.[62] The imposition of a rule without providing adequate

---

[58] NPRM at 83851-52.

[59] *State Farm*, 463 U.S. at 43 (citing *Burlington Truck Lines v. United States*, 371 U.S. 156, 168 (1962)); *see also DHS v. Regents of Univ. of Cal.*, 140 S. Ct. 1891, 1912-13 (2020).

[60] It is a basic premise of administrative law that an agency must "pay[] attention to the advantages *and* disadvantages of agency decisions," *EPA*, 576 U.S. at 753 (emphasis in original), and cannot "entirely fail[] to consider an important aspect of the problem" before the agency, *State Farm*, 463 U.S. at 43.

[61] *See Greater Yellowstone Coal., Inc. v. Servheen*, 665 F.3d 1015, 1030 (9th Cir. 2011) (agency cannot ignore evidence "pointing in the opposite direction" from its conclusions); *see also Dep't of Commerce v. New York*, 139 S. Ct. 2551, 2575 (2019) ("[T]he evidence tells a story that does not match the explanation the Secretary gave for his decision.").

[62] The NPRM rightly notes that the APA "requires publication of the final version of a rule at least thirty days before the rule's effective date" (*see* 5 U.S.C. § 553(d)), but in the next sentence concludes that this requirement (and others) "do not apply." NPRM at 83852.

time for compliance is arbitrary and capricious.[63] This is especially true when the agency has shown no particular need for extraordinary urgency (as here, *see* Section I).[64] Indeed, FinCEN's extensive discussion of the BSA status of self-hosted wallets in its May 2019 guidance shows that it has been aware of issues related to self-hosted wallets for some time.[65]

Here, compliance with the Proposed Rule's requirements demands the creation of complex technical systems needed to collect, potentially verify, and protect sensitive personal information about individuals who are not customers of the exchanges. While Covered Entities attempt to build such systems in a secure manner, they will be required to completely prohibit transactions with self-hosted wallets. During that interval, customers are likely to flee to exchanges overseas to meet their needs, and may not return, exacerbating the negative effects described above in Section V. Failure to allow Covered Entities time to implement measures required by any final rule is therefore arbitrary and capricious.

This point—the specific time and burdens required to build the technical systems required to manage compliance with the proposed rule—is one on which the public also would have been able to provide detailed comments had it had a longer comment period. It is also one area the private sector is likely able to judge more accurately than FinCEN. But with six business days and during the holidays, it was impossible to provide such complex analyses.

Second, the Proposed Rule—and its aggressive implementation schedule—seriously erodes the "significant reliance interests" of cryptocurrency exchanges that have organized themselves around the existing regulatory framework.[66] Instead of simply requiring cryptocurrency exchanges to verify the identity of their own *customers*—a requirement that is common to different types of financial institutions pursuant to the BSA—the Rule would require them to identify and potentially verify the *counterparties* of their customers. In no other context do FinCEN's regulations implementing the BSA impose an obligation similar to what is set out in the NPRM, which is impossible for cryptocurrency exchanges subject to the BSA to comply with at this time because of the need to create the technical systems described above. The

---

[63] *See Am. Fed. of Labor & Congress of Indus. Orgs. v. Chao*, 298 F. Supp. 2d 104, 126-28 (D.D.C. 2004), *rev'd on other grounds*, 409 F.3d 377 (D.C. Cir. 2005) (holding that the imposition of an effective date less than two months after the issuance of a rule was arbitrary and capricious because it required plaintiffs to make "far-reaching changes" to comply with the rule, such as developing new accounting systems, purchasing new computers and software, and training staff).

[64] *Chao*, 298 F. Supp. 2d at 127.

[65] FINCEN, FIN-2019-G001, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 14-16 (2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[66] *Encino Motorcars, LLC v. Navarro*, 136 S. Ct. 2117, 2126 (2016); *see also, e.g.*, *Regents of Univ. of Cal.*, 140 S. Ct. at 1915 ("[B]ecause DHS was not writing on a blank slate, it was required to assess whether there were reliance interests, determine whether they were significant, and weigh any such interests against competing policy concerns.").

Proposed Rule will thus force cryptocurrency exchanges to halt transactions with self-hosted wallets, which will lead to an immediate loss of revenue for the exchanges and a breach of trust between exchanges and their customers. This would significantly impair reliance interests.

CONCLUSION

a16z has a substantial interest in ensuring that cryptocurrency is regulated in a well-reasoned and procedurally sound manner. Respectfully, the proposed rule is neither. It represents a rushed and ill-advised regulation that would have many foreseeable and unintended consequences. Blockchain-based systems hold enormous promise to deliver innovative products and services to the global financial system, including for those who have historically existed outside it or at its margins.

Instead of proposing a rule that is based on reliable evidence of regulatory need; that grapples with the difficult tradeoffs in regulating this activity; and that proposes mechanisms of public/private partnership that can actually assist the fight against financial crime, FinCEN has instead proposed a rule at the eleventh hour of an outgoing administration that has all the hallmarks of arbitrary and capricious agency action. The NPRM fails to establish a close relationship between the facts the agency has purportedly found and the rule it proposes to adopt; it sweeps in commercial activity far beyond the self-hosted wallets with which FinCEN purports to be concerned; key components of the proposed rule are vague and will be very challenging to implement; FinCEN ignores foreseeable negative impacts of its proposed rule; and FinCEN has bypassed standard notice and comment processes without cause, over the holiday season. For these reasons, FinCEN should withdraw its proposed rule or extend the comment period for an additional 60 days so that it can engage in a meaningful consultation with industry about topics that are vital to the future of the U.S. economy.

Respectfully submitted,

/s/ Katie Haun

Katie Haun
General Partner, a16z

/s/ Anthony Albanese

Anthony Albanese
Operating Partner, a16z

Cc: Counsel to a16z on this matter:

(1) Wilmer Cutler Pickering Hale and Dorr LLP

Kelly P. Dunbar, Esq.
Ari Holtzblatt, Esq.
Zachary K. Goldman, Esq.

(2) Eugene Volokh, Esq.