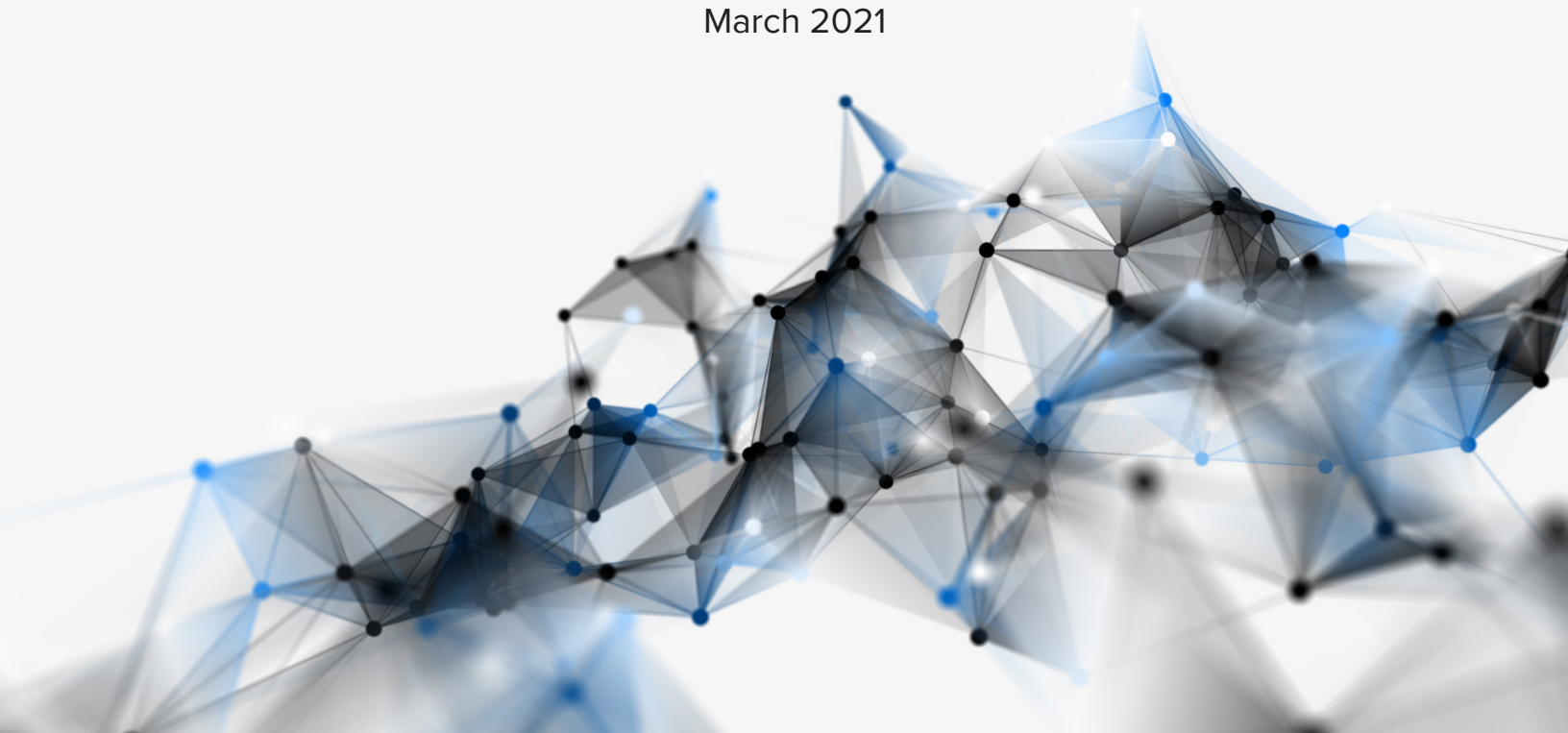
BLOCKCHAIN ASSOCIATION

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

March 2021



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

March 29, 2021

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

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

To whom it may concern:

The Blockchain Association submits these additional comments in response to the Notice of Proposed Rulemaking (the "NPRM") titled "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets."[1] The Blockchain Association (the "Association") is a not-for-profit organization dedicated to improving public policy in ways that will help public blockchain networks and their users develop and prosper in the United States. It endeavors to educate policymakers, courts, and the public about the inner workings of distributed ledgers and how regulatory clarity can bring about a more secure, competitive, and innovative digital marketplace. The Association is comprised of industry leaders who are committed to responsibly developing and supporting blockchain networks fueled by cryptocurrencies. Its diverse membership reflects the complexity of this dynamic market and includes projects that contribute to distributed networks, trading platforms that allow users to exchange cryptocurrencies, and early stage investors that support the entire ecosystem. Given its diverse membership, the Blockchain Association is well positioned to provide the Financial Crimes Enforcement Network ("FinCEN") and the Department of the Treasury with the perspectives of those who facilitate and engage in transactions of "convertible virtual currency" ("CVC") or "digital assets with legal tender status" ("LTDA") involving "unhosted wallets." The Blockchain Association thanks FinCEN for its extension of the extremely truncated comment period initially provided to the public and for its good faith engagement with the industry since the publication of this NPRM. We share FinCEN's objectives of protecting our national security and disrupting illicit activity and malicious actors. The Blockchain Association's membership stands ready and willing to work with regulators to accomplish these objectives in a manner that will ensure the United States remains at the forefront of financial innovation in the 21st century.

---

[1] 85 Fed. Reg. 83,840 (Dec. 23, 2020), *available at*: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf.

The Association agrees that the goals of the proposed requirements are "essentially equivalent" to the goals of the reporting requirements for cash transactions ≥$10,000, but given the unique features of transparent blockchain networks, a recordkeeping requirement in the cryptocurrency ecosystem would more effectively accomplish the NPRM's objectives. The January 15th extension notice states that the "proposed [reporting] requirements [for digital transactions, which FinCEN intends to call value transaction reports ("VTRs")] are essentially equivalent to the existing [currency transaction report ("CTR")] reporting requirements that apply to transactions in currency."[2] The January 15th extension notice also asserts that "the proposed rule is a vital loophole-closing measure to prevent illicit transactions using CVC and LTDA, including the financing of terrorism, in light of the fact that such transactions would otherwise be subject to familiar and long-established reporting requirements if they were in cash."[3] While the Association applauds FinCEN's effort to bring the cryptocurrency and blockchain industry into the regulatory fold, a recordkeeping requirement would not only accomplish law enforcement objectives but also better balance other priorities such as respecting innocent users' privacy. The remainder of this comment letter will explore why a recordkeeping requirement would effectively and efficiently accomplish the goals set forth in the NPRM. This letter does not address the proposed collection of counterparty information as described in both the December 23, 2020 and January 15, 2021 notices. For the reasons explained in its January 4th comment letter to FinCEN,[4] the Association remains vehemently opposed to an unprecedented counterparty identification requirement in any form.

I. Executive Summary

Without a reporting requirement in the cash ecosystem, law enforcement would have no knowledge whatsoever of ephemeral, anonymous cash transactions. A recordkeeping requirement for financial institutions ("FIs") in the traditional cash ecosystem would therefore be useless to law enforcement because, without a central repository of transaction information created by a reporting requirement, law enforcement could not identify suspicious transaction activity. In practice, without a reporting requirement in the cash ecosystem, there would be no method to identify which FIs' records would be germane to an investigation. The same limitation is not present in the transparent blockchain cryptocurrency ecosystem, however.

Transparent blockchains eliminate the need for a reporting requirement and the centralized database of transaction information that it creates for law enforcement because—for

---

[2] 86 Fed. Reg. 3897 (January 15, 2021), *available at*: https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf

[3] Ibid.

[4] Blockchain Association, "Comment on FR Doc # 2020-28437" (January 4, 2021), *available at*: https://www.regulations.gov/comment/FINCEN-2020-0020-6578.

every transaction—they already aggregate the information that law enforcement needs to identify and trace suspicious activity. Transparent blockchains create an immutable record of every transaction ever made by users of a given network, a public record that already includes six of the eight data points that the NPRM proposes to be included in the VTR. Law enforcement can use this record to first identify suspicious transactions involving FIs and then obtain personally identifiable information (PII) from the relevant institution, a system that would also help address the severe security and privacy concerns raised in the over 7,000 comments FinCEN has received on this NPRM.[5]

While a traditional CTR notifies law enforcement that a transaction has occurred and provides law enforcement with information about a single financial transaction at a distinct moment in time, the filing of just one of the VTRs proposed in the NPRM would provide the government with the ability to centralize and surveil, in real time, *every* transaction—past, present, and future—an American citizen makes on a transparent blockchain. Tying one's identity to their public address on a public blockchain allows for the aggregation of one's entire financial life and would represent a gross invasion of one's privacy. In the cash ecosystem, this surveillance power would equate to the filing of a CTR for every single cash transaction a citizen has ever conducted or will ever conduct regardless of the amount of money involved in the transaction. In addition, the proposed VTR requirement would centralize this very sensitive information, creating a data "honey pot" that represents a new and significant financial incentive for hostile actors, both criminal and nation-state. Ultimately, the Association believes that such surveillance power does not strike the right balance between providing useful information to law enforcement while respecting the privacy rights of individuals. By contrast, a pure recordkeeping requirement substantially reduces these privacy and security risks while still ensuring law enforcement has access to relevant investigatory information. Under this type of requirement, very sensitive PII would be distributed among individual FIs, which are charged with protecting their own customers' security, while the information would be retained and available for law enforcement purposes.

Additionally, because transparent blockchains create an immutable, public, and searchable record of all transactions in a given cryptocurrency—a feature cash lacks—a pure recordkeeping requirement at the ≥$10,000 threshold would provide law enforcement with more information than traditional cash CTRs. Having received PII records about a party involved in a suspicious transaction, law enforcement would have access to *every* financial transaction the transacting party has made and will make, which is an enormous amount of information well beyond what is included in a single traditional CTR. However, because such identifying information would be revealed to law enforcement pursuant to the identification on a transparent blockchain of a suspicious transaction involving an FI, a pure recordkeeping requirement better

[5] Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," (December 22, 2020), *comments available at*: https://www.regulations.gov/document/FINCEN-2020-0020-0001/comment.

balances the privacy rights of citizens while still providing an enormous amount of information to law enforcement in the course of investigations.

Another benefit of a recordkeeping requirement is that it avoids inundating FinCEN with an enormous amount of highly sensitive information, the vast majority of which would be related to completely innocuous transactions. The unique characteristics of the cryptocurrency ecosystem almost guarantees that FIs would file VTRs for transactions well beyond the written parameters of the NPRM, producing a deluge of useless and duplicative, but highly sensitive, information. In the cash ecosystem, many have raised concerns that CTRs are generally not useful to law enforcement as they are not based on any identified suspicion, just on transactions meeting a certain threshold. Indeed, the CTR is currently being scrutinized, in part due to the abundance of innocuous customer information that it produces. The Anti-Money Laundering Act of 2020 (the "AMLA") mandates that the Treasury conducts several studies related to the efficiency of Bank Secrecy Act ("BSA") reporting requirements, including CTRs and suspicious activity reports ("SARs"). These reviews, two of which will be completed by January 2022, will provide information squarely relevant to this rulemaking, such as the rate at which law enforcement uses CTRs to advance investigations. Waiting to proceed with this rulemaking until those reviews are complete will lead to a more effective, informed rulemaking.

II. Because transparent blockchains create an immutable, public, and searchable record of all transactions in a given cryptocurrency, a recordkeeping requirement accomplishes the NPRM's objectives by ensuring all relevant transaction information is retained and available for law enforcement purposes.

Cryptocurrencies based on distributed ledgers enable the direct transfer of assets—both monetary and otherwise—over the internet. Before the invention of bitcoin in 2008, digital transactions required the services of intermediating third-parties like banks. Without a trusted third-party intermediary keeping a ledger of account holders' balances and vouching for both parties to a transaction, transacting parties could not transact digitally. Accordingly, there was no secure way to engage in "peer-to-peer" transactions over the internet, i.e. transactions that could be initiated and completed without the permission or aid of a third-party financial institution.[6] To achieve the ability to transact over the internet without the participation of intermediaries, cryptocurrency networks employ distributed ledgers to keep a record of transactions in a given cryptocurrency. The history of transactions is securely recorded in digital format through the use of cryptography and a ledger-like data structure called a "blockchain." This secure history of transactions allows individuals to confidently transact without needing an intermediating third-party to vouch for either party to the transaction. The protocol, and the decentralized network of computers that run it, facilitate transactions that are valid. To direct and validate

[6] Peter Van Valkenburgh, *Electronic Cash, Decentralized Exchange, and the Constitution*, Coin Center (March 2019) *available at*: https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/.

transactions, users of cryptocurrency networks employ “public addresses” and “private keys.”[7] A private key is cryptographically linked to a public address, and the private key allows one to control the digital assets associated with the public address.[8] Access to a private key is the *only* way to exercise control over digital assets associated with a public address. Loss of the private key generally means the digital assets associated with the public address are forever lost, and anyone with the key can exercise control over the assets associated with the public address. Public address and private key pairs can be generated costlessly by any entity who has an internet connection and thus access to the open source software that fuels these digital transaction networks.

While cryptocurrencies leverage distributed ledgers and public address/private key cryptography to approximate the peer-to-peer transactability of cash, there are key differences between cash and cryptocurrencies that should be considered in the context of this rulemaking. First, unlike cash, sending high-value cryptocurrency transactions does not require additional cost or effort for the transacting parties. The parties, using their computers or mobile phones, simply indicate how much value to send from their public address to another public address. With cash transactions, however, the larger the transaction, the more physical currency is required in order to complete the value transfer. Additionally, cash must be physically moved to complete the transaction, which requires additional time and resources that are not required in cryptocurrency transactions. Second, cryptocurrencies can be “programmed” to restrict who can hold them, how they can be sent, when they can be sent, etc., a feature cash lacks. A simple example of the

---

[7] A simple analogy to public addresses are email addresses: pseudonymous identifiers that allow one to send and receive emails. Private keys similarly can be thought to act like email passwords that must be produced each time one wishes to send an email.

[8] A “self-hosted” or “unhosted” wallet refers to when the private key for a particular public address are held by the natural beneficial owner of the assets associated with the public address. “Smart contracts" are also identified by public addresses but operate differently. For example, there are two types of accounts on the Ethereum network: 1) Externally Owned Accounts (EOA) and 2) Contracts Accounts. EOAs refer to the “typical” public blockchain addresses that have associated private keys managed by a user of the network. Smart contracts operate differently. Smart contracts are just computer programs. Every smart contract is bound to a contract account public address. The code of a smart contract is executed when that specific contract public address is called as part of a transaction message. In this manner, a contract account is not managed by a private key (like an EOA address). Instead, the smart contract runs in response to a transaction/message from EOAs or other contract accounts. A simple analogy is to a vending machine—they do not operate except for when a user puts a dollar in. All that being said, many smart contract developers build code that may allow certain addresses to have special administrative functions (e.g., changing the parameters of the code in the smart contract or even shutting the contract down completely), but this code does not change the fact that smart contracts only respond to external messages. Addresses with special administrative privileges could be controlled by a single person or could be another smart contract that sends messages based on the votes of, for example, governance token holders. Finally, smart contracts can have no administrative address at all, making them completely open-source and unchangeable.

programmability of cryptocurrencies are multi-signature wallets.[9] Third, unlike fiat currencies, cryptocurrencies are not legal tender anywhere in the world and are not widely accepted for retail use, paying taxes, or settling debts, so they must usually exit into fiat and fiat's surveillance regime. Finally and critically, cash transactions are inherently anonymous and ephemeral, while cryptocurrencies with transparent blockchains reveal the transaction history of cryptocurrencies and their pseudonymous users.

Because cash transactions are inherently ephemeral and anonymous, the only method through which law enforcement can access information about a cash transaction is surveillance. Given these unique features of cash and the central importance of payments to all economic activities, licit and illicit, the BSA deputizes FIs and other entities to conduct financial surveillance of cash transactions on the government's behalf, responsibilities that include filing currency transaction reports (CTRs) for cash transactions ≥$10,000.[10] Without these CTRs, law enforcement would have *no knowledge whatsoever* of these cash transactions, including their existence at all; cash's ephemeral and anonymous nature creates this "invisibility." There would be "nothing to go on," no entity to subpoena, no transaction history to examine, etc.

Transparent blockchains, on the other hand, eliminate the need for a reporting requirement and the centralized database of information that it creates for law enforcement because they already aggregate the information that law enforcement needs to identify and trace suspicious transactions. Unlike cash transactions, transparent blockchains create a permanent ledger of every transaction ever conducted using a given cryptocurrency—in addition to the balances associated with every address on the network—regardless of whether a BSA-obligated entity is party to the transaction or not. Indeed, six of the eight pieces of information listed in the NPRM are already publicly available and searchable on transparent blockchains for every transaction, including (1) the type of virtual currency used, (2) the date and time of the transaction, (3) the amount of the transaction, (4) the value of the transaction in USD, (5) the transaction hash, and (6) the transacting public addresses.[11] Herein lies one of the key differences between the cash and cryptocurrency ecosystems that ultimately justifies the implementation of a recordkeeping, not a reporting requirement, in the cryptocurrency ecosystems.

Because transparent blockchains essentially create a public and pseudonymous CTR database for every transaction, a recordkeeping requirement for transactions ≥$10,000 involving

---

[9] For a basic introduction to multi-signature wallets and their role in cryptocurrency transactions, please see: Ben Davenport, "What is multi-sig, and what can it do?," *Coin Center* (January 1, 2015), *available at*: https://www.coincenter.org/education/advanced-topics/multi-sig/.

[10] 31 CFR 1010.311, *available at*: https://www.govinfo.gov/content/pkg/CFR-2020-title31-vol3/pdf/CFR-2020-title31-vol3-part1010.pdf.

[11] For an example of the information transparent blockchains immutably record on a public ledger, please see: https://blockstream.info/tx/b9657c5cd8b255b8e5647a7c977ffdd589a61f307034ff0eb55bb30463094973.

self-hosted wallets ensures FIs could produce identifying information after law enforcement identifies a suspicious transaction. In other words, using the searchability of transparent blockchains, FinCEN and law enforcement would be able to identify transactions that warrant additional scrutiny, and with the recordkeeping requirement in place, know that the information required to pursue investigations would be preserved and accessible at financial institutions.

One of the concerns that law enforcement might have about this proposed recordkeeping requirement is that the lack of an identity-based CTR database in the cryptocurrency ecosystem would fail to provide law enforcement with the ability to detect an unknown cryptocurrency nexus to unrelated suspicious activity. The identity-based SAR database, which provides law enforcement with risk-based information for suspicious transactions at lower thresholds than the CTR, as well as Section 314(a) of the USA PATRIOT ACT of 2001,[12] ultimately address this concern without the need for an identity-based CTR database. Should an initial query of a risk-based SAR database fail to produce useful information for law enforcement, FinCEN's regulations[13] under Section 314(a) "enable federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 34,000 points of contact at more than 14,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering… Through an expedited communication system, FinCEN's 314(a) process enables an investigator to canvas the nation's financial institutions for potential lead information that might otherwise never be uncovered. This cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralized and rapidly evaluated."[14]

III. A recordkeeping requirement avoids unnecessarily inundating FinCEN with a significant amount of highly sensitive "white noise."

A recordkeeping requirement not only ensures all relevant information is retained and available for law enforcement but also avoids unnecessarily inundating FinCEN with a significant volume of highly sensitive "white noise" about innocuous financial transactions, a phenomenon currently created by existing CTR reporting requirements. While FinCEN recently estimated that it receives 16,087,182 CTRs per annum,[15] the rate at which CTR filings are useful to law enforcement is not publicly available to the Association's knowledge. However, an examination of FinCEN's

---

[12] Public Law No. 107-56, *available at*: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

[13] Financial Crimes Enforcement Network, "FinCEN's 314(a) Fact Sheet" (February 23, 2021), *available at*: https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.

[14] Financial Crimes Enforcement Network, "FinCEN's 314(a) Fact Sheet" (February 23, 2021), *available at*: https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.

[15] 85 Fed. Red. 45,959 (July 30, 2020), *available at*: https://www.govinfo.gov/content/pkg/FR-2020-07-30/pdf/2020-16481.pdf.

use of SARs—risk-based filings that would logically produce more relevant information for law enforcement than a threshold based reporting requirement—reveals that even risk-based filings are largely "white noise." According to *Buzzfeed News*, in 2019 FinCEN received more than 2,000,000 SARs.[16] Public testimony suggests that FinCEN reviews about 50 of these SARs per day, which amounts to the review of only about 18,250 SARs per year.[17] In other words, FinCEN did not review approximately 99.1% of the risk-based SARs it received in 2019. Because the proposed VTRs would be filed based on transaction thresholds instead of risk assessments,[18] it is safe to assume that the proposed VTR system, like the existing CTR system, would result in FinCEN receiving a vast amount of highly sensitive information related to innocent transactions. Such information is useless to law enforcement. To make matters worse, in the cryptocurrency ecosystem, the proposed reporting requirement would likely be even more inefficient at producing relevant information than the existing CTR system.

Fundamental characteristics of the cryptocurrency ecosystem and the NPRM's vagueness will force FIs to vastly overreport information to FinCEN beyond the already expansive requirements delineated in the NPRM. At this time, FinCEN has proposed to exempt transactions between hosted wallets from the reporting requirement, which means that only transactions ≥$10,000 between an FI and a self-hosted wallet will fall under the proposed reporting requirement. This exemption will have a limited effect, however, because FIs generally cannot determine with consistent confidence whether the counterparty to a transaction is interacting with cryptocurrencies through an FI, i.e. through a hosted wallet, or directly on their own behalf, i.e. through a self-hosted wallet. As such, a conservative approach to the NPRM's proposed reporting requirement would demand that FIs file VTRs for every external transaction that meets the ≥$10,000 threshold, which would greatly increase the number of reports that an FI would have to report, in turn increasing the volume of highly sensitive "white noise" delivered to FinCEN.[19] The continued growth of the cryptocurrency ecosystem will only exacerbate this situation. Moreover, the NPRM's requirements are explained using terms that have never been formally defined in laws or regulations and are not specifically defined by the NPRM, including critical terms such as "unhosted wallet," "convertible virtual currency," and "legal tender digital assets." Faced with a new requirement predicated on undefined terms, a conservative approach

---

[16] Leopold, Jason, Anthony Cormier, John Templon, Tom Warren, Jeremy Singer-Vine, Scott Pham, Richard Holmes, et al. "FinCen Files." New York, N.Y.: BuzzFeed News, September 20, 2020. https://www.buzzfeednews.com/fincen-files.

[17] K. A. Blanco, *Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement* (June 12, 2019), *available at*: https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-lawprogram-corporate-compliance-and.

[18] 85 Fed. Reg. 83,840 (Dec. 23, 2020), *available at*: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf.

[19] Payward, Inc., "Comment on FR Doc #2020-28437" (January 4, 2021), *available at*: https://www.regulations.gov/comment/FINCEN-2020-0020-6190.

would likewise compel FIs to report transactions well beyond those FinCEN may be intending to capture.

IV. A recordkeeping requirement effectively balances providing law enforcement with useful information with respecting innocent users' right to privacy and security, thus addressing the core concerns raised in the over 7,000 comments FinCEN has received on this NPRM.

A recordkeeping requirement that avoids inundating FinCEN with highly sensitive "white noise" not only accomplishes law enforcement objectives but also better protects users' privacy and security. The proposed VTR requirement, which is based on a monetary threshold rather than a determination of potential criminal activity, would primarily capture innocent conduct, aggravating the privacy and security concerns associated with the proposed reporting requirement. On the other hand, a recordkeeping requirement would mitigate these concerns by decentralizing retention of this information at individual financial institutions.

A. A recordkeeping requirement mitigates severe privacy concerns.

As previously mentioned, once a public address is attributed to an individual's identity, an individual's transaction history can be reconstructed and future transactions can be traced. Therefore, the filing of just one of the proposed VTRs would provide the government with unfettered access to all of a public address owner's past, present, and future transactions on a network. In the traditional cash ecosystem, this reporting requirement would be akin to requiring the filing of a CTR for every cash transaction a citizen has ever engaged in or will ever engage in, regardless of the transaction amount or whether a FI is involved in the transaction. This level of surveillance would vastly exceed the amount of information the government currently obtains with respect to fiat transactions and would invade the privacy of American citizens.

The reporting regime put forth in the NPRM would unnecessarily violate the financial privacy of users and "would transform a regulatory regime designed to prevent financial institutions from using privacy as a shield for complicity in their customers' illicit activity into a tool of general surveillance."[20] The Blockchain Association believes that most Americans would view the government's ability to track every financial transaction they make without appropriate legal process as a profound invasion of privacy. Indeed, Chairman of the Board of Governors of the Federal Reserve Jerome Powell has testified that, "...the idea of having a ledger where you know everybody's payments, that's not something that would be particularly attractive in the United

[20] Jaikumar Ramaswamy, "Comment on FR Doc #2020-28437 (January 4, 2021), *available at*: https://www.regulations.gov/comment/FINCEN-2020-0020-6556.

States…"[21] One need only look to the 7,000 comments FinCEN received on this NPRM as further evidence of this view.[22]

While there are good reasons to report certain transactions, such as when suspicious activity is detected or when a transaction may be completely ephemeral, enabling the total surveillance of law abiding citizens' financial activities in real time could not be justified even in a situation where the reports are likely to be consistently useful to law enforcement (which as noted before, is the not case with respect to this NPRM because a recordkeeping requirement would accomplish the goals of the NPRM). In addition to better balancing law enforcement needs with the privacy rights of innocent American citizens, the recordkeeping requirement would also mitigate security concerns associated with the aggregation and centralization of Americans' financial activity.

B. A recordkeeping requirement mitigates security concerns.

The proposed VTR database creates significant security concerns because it would aggregate information that could unmask citizens' entire financial lives on transparent blockchains into a single, hackable database. This database would be an extremely attractive "honeypot" for malicious actors, nation-state and criminal, which is particularly concerning given the recent string of successful attacks targeting U.S. government networks. In the last few years, cyberattacks have plagued U.S. government systems. Indeed, hackers have managed to pull-off several unprecedented attacks including the U.S. Office of Personnel Management ("OPM") data breach[23] and the recent Solarwinds hack, which reportedly implicated the Departments of State, Energy, Commerce, Justice, Defense, Treasury, and Homeland Security.[24] This data insecurity is particularly concerning because the exposure of PII collected as a result of this NPRM's requirements could have especially devastating effects. A leak of such PII would link a person's real-world identity with a formerly pseudonymous wallet address, painting a "bullseye" on the wallet holder and making them the potential target of a variety of criminal activities, including

---

[21] House Hearing Serial Number 116-85, *Monetary Policy and the State of the Economy: Hearing Before the Committee on Financial Services*, 116th Congress, Second Session (February 11, 2020), *available at*: https://financialservices.house.gov/uploadedfiles/chrg-116hhrg42819.pdf.

[22] Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," (December 22, 2020), *comments available at*: https://www.regulations.gov/document/FINCEN-2020-0020-0001/comment.

[23] Office of Personnel Management Cybersecurity Resource Center, "Cybersecurity Incidents," *available at*: https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[24] Isabella Jibilian and Katie Canales, "Here's a Simple Explanation of How the Massive SolarWinds Hack Happened and Why It's Such a Big Deal," *Business Insider* (February 25, 2021), *available at*: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

identity theft, robbery, and kidnapping.[25] Beyond creating risks for individuals, mass data breaches can create national security risks, as evidenced by the fallout from the OPM breach.[26] While a compelling need of law enforcement and a lack of available alternatives might justify such security risks, both justifications are lacking in this instance due to the workability and effectiveness of a recordkeeping requirement. As such, a reporting requirement unnecessarily creates a database of highly sensitive PII that would become an obvious target for attackers, while the decentralization of sensitive PII at individual FIs would mitigate these security risks and concerns.

V. Not only should FinCEN wait for the findings of centrally relevant reviews mandated by the Anti-Money Laundering Act of 2020 to proceed with this rulemaking, but also a recordkeeping requirement would better align with the goals of the AMLA and FinCEN's broader AML/CFT modernization effort.

The U.S. government is in the midst of a major review and overhaul of the national AML/CFT regime. Congress's enactment of the AMLA in January 2021 and FinCEN's September 2020 advanced notice of proposed rulemaking (ANPRM)[27] evidence that reform is coming to the United States' AML/CFT regime. With such change imminent, regulators should be wary of hurriedly introducing a reporting rule that will be improved and informed by the findings of the various reporting requirement reviews currently underway, two of which will be completed by January 2022.

A. FinCEN should wait to proceed with this rulemaking until it completes several policy reviews mandated by Congress that are germane to key issues posed by this rulemaking.

At Congress's direction in the AMLA, the Treasury is about to undertake several analyses of BSA reporting requirements across the entire financial sector, including CTRs. The Association believes it would be highly valuable to delay proceeding with this rulemaking until these studies are complete, the learnings can be shared with industry, and the findings can be applied to this proposed rulemaking. In the AMLA, Congress directs the Treasury to study the efficacy, weigh the

---

[25] Nathaniel Popper, "Bitcoin Thieves Threaten Real Violence for Virtual Currencies," *The New York Times* (February 18, 2018), *available at*: https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html.

[26] Zach Dorfman, "China Used Stolen Data To Expose CIA Operatives in Africa and Europe," *Foreign Policy* (December 21, 2020), *available at*: https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.

[27] The Financial Crimes Enforcement Network, "Anti-Money Laundering Program Effectiveness," *Advanced Notice of Proposed Rulemaking* (September 17, 2020), 85 Fed. Reg. 58023, *available at:* https://www.federalregister.gov/documents/2020/09/17/2020-20527/anti-money-laundering-program-effectiveness.

costs and benefits, and re-examine the thresholds of its current reporting requirements to ensure the information provided is both useful to law enforcement and reduces any unnecessary burden for obligated financial institutions. Through the analyses mandated by the AMLA (three of which review CTR filings), Congress seeks to understand, in part: i) how reported information is actually used (i.e., frequency of new leads, arrests etc.),[28] ii) whether to modify current thresholds,[29] iii) whether reporting burdens can be reduced by eliminating reports with little or no value,[30] iv)

[28] Section 6204 of the AMLA directs the Secretary of the Treasury to "...undertake a formal review of the financial institution reporting requirements relating to currency transaction reports..." The review will include an analysis of, in part, "the fields on the currency transaction report form, and whether the number or nature of the fields on those forms should be adjusted; the categories, types, and characteristics of... currency transaction reports that are of the greatest value to, and that best support, investigative priorities of law enforcement and national security agencies; the increased use or expansion of exemption provisions to reduce currency transaction reports that may be of little or no value to the efforts of law enforcement agencies;... the current financial institution reporting requirements under the Bank Secrecy Act and regulations and guidance implementing the Bank Secrecy Act;... [and] the appropriate manner in which to ensure the security and confidentiality of personal information." (AMLA 1182) Treasury must complete and publish this report next January and propose rulemakings that implement the findings of the report. Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

[29] Section 6205 of the AMLA directs the Secretary of the Treasury to "...review and determine whether the dollar thresholds, including aggregate thresholds, under sections 5313, 5318(g), and 5331 of title 31, United States Code, including regulations issued under those sections, should be adjusted."# (AMLA 1183) The review is required to consider "(A) the effects that adjusting the thresholds would have on law enforcement, intelligence, national security, and homeland security agencies; (B) the costs likely to be incurred or saved by financial institutions from any adjustment to the thresholds; (C) whether adjusting the thresholds would better conform the United States with international norms and standards to counter money laundering and the financing of terrorism; (D) whether currency transaction report thresholds should be tied to inflation or otherwise be adjusted based on other factors consistent with the purposes of the Bank Secrecy Act; (E) any other matter that the Secretary determines is appropriate." (AMLA 1183-84). Treasury must complete and publish this report next January and propose rulemakings that implement the findings of the report. Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

[30] Section 6205 of the AMLA directs the Secretary of the Treasury to "...review and determine whether the dollar thresholds, including aggregate thresholds, under sections 5313, 5318(g), and 5331 of title 31, United States Code, including regulations issued under those sections, should be adjusted." (AMLA 1183) The review is required to consider "(A) the effects that adjusting the thresholds would have on law enforcement, intelligence, national security, and homeland security agencies; (B) the costs likely to be incurred or saved by financial institutions from any adjustment to the thresholds; (C) whether adjusting the thresholds would better conform the United States with international norms and standards to counter money laundering and the financing of terrorism; (D) whether currency transaction report thresholds should be tied to inflation or otherwise be adjusted based on other factors consistent with the purposes of the Bank Secrecy Act; (E) any other matter that the Secretary determines is appropriate." (AMLA 1183-84). Treasury must complete and publish this report next January and propose rulemakings that implement the findings of the report. Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

whether the current system adequately maintains security and confidentiality of personal information,[31] and v) costs imposed on the industry.[32]

Undoubtedly, the findings of these reviews will substantially inform the rulemaking at hand in that the insights gleaned from these reviews will help regulators craft more effective policy that benefits all relevant parties. Not only will the learnings from these studies benefit the private sector by revealing which BSA requirements efficiently deliver useful information to law enforcement, but the Treasury itself will also certainly have new views and information related to the utility of reporting requirements following these surveys. Therefore, FinCEN, in an effort to bring into force an effective rulemaking that efficiently leverages the resources of all parties, should wait until at least the delivery of the January 2022 reports before proceeding with this rulemaking. Moreover, the Blockchain Association's members hope to avoid building new reporting or recordkeeping infrastructure only to potentially revisit and rebuild these systems next year.

More generally, the proposed reporting requirement ultimately belies Congress's intent and goals for the AMLA. Through this law, Congress, seeks to, in part, "...encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism, [and] to reinforce that the anti-money laundering and countering the financing of terrorism policies, procedures, and controls of financial institutions shall be risk based."[33] The Blockchain Association does not believe that the NPRM's extension of a blunt, threshold-based, and invasive reporting requirement into the most innovative sector in financial services successfully leverages the unique characteristics of transparent blockchains to "more effectively counter money laundering and the financing of

---

[31] Section 6216 of the AMLA directs the Secretary of the Treasury to "...undertake a formal review of the regulations implementing the Bank Secrecy Act and guidance related to that Act..."# including the identification of "...those regulations and guidance that may be outdated, redundant, or otherwise do not promote a risk-based anti-money laundering compliance and countering the financing of terrorism regime for financial institutions..." The Treasury must submit this report to Congress next January after consideration of public comment. In addition, Congress directs the Treasury to "...make appropriate changes to..." BSA regulations and guidance to, in part, "...improve, as appropriate, the efficiency of those provisions." Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

[32] Section 6504 of the AMLA directs the Comptroller General of the United States to "...commence a study of currency transaction reports, which shall include a review... of the effectiveness of the currency transaction reporting regime... an analysis of the importance of currency transaction reports to law enforcement, and an analysis of the effects of raising the currency transaction report threshold." This study, which will also include "recommendations for improving the currency transaction reporting regime, must be submitted to Congress not later than December 31, 2025." Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

[33] Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

terrorism"[34] in the cryptocurrency ecosystem. Nor does the Blockchain Association believe that the adoption of a threshold-based reporting requirement advances Congress's intent to reinforce a risk-based approach to AML/CFT obligations. On the other hand, the recordkeeping requirement proposed herein would 1) leverage new technology (transparent blockchains) to identify suspicious activity and 2) deliver risk-based information to law enforcement, better aligning with Congress's intent and FinCEN's efforts to modernize the national BSA/CFT regime.

B. A recordkeeping requirement aligns with FinCEN's current effort to modernize the national AML regime.

A recordkeeping requirement that avoids inundating FinCEN with excessive and largely duplicative information aligns with FinCEN's current effort "to modernize the national AML regime." In September 2020, FinCEN released an advanced notice of proposed rulemaking (ANPRM) seeking "public comment on potential regulatory amendments to establish that all covered financial institutions subject to an anti-money laundering program requirement must maintain an effective and reasonably designed anti-money laundering program."[35] FinCEN's objectives for this effort are, in part, to "place a greater emphasis on providing information with a high degree of usefulness to government authorities,"[36] "to maximize efficiency, quality, and speed of providing data to government authorities,"[37] and to provide "due consideration for privacy and data security."[38]

The recordkeeping framework proposed in this letter would meet these objectives more closely than a threshold-based reporting requirement. Not only would it ensure that transparent and public blockchains are used by law enforcement as a tool that maximizes the "efficiency, quality, and speed" of data collection, but also it would better respect Americans' right to "privacy and data security" by facilitating the decentralized aggregation of Americans' personal information at their financial institutions. In the context of these vital considerations, a recordkeeping requirement represents a viable alternative that satisfies the needs of all relevant parties, i.e. government, law enforcement, private industry, and the American public.

VI. Conclusion

---

[34] Public Law No. 116-283, *available at:* https://www.congress.gov/bill/116th-congress/house-bill/6395/text/.

[35] The Financial Crimes Enforcement Network, "Anti-Money Laundering Program Effectiveness," *Advanced Notice of Proposed Rulemaking* (September 17, 2020), 85 Fed. Reg. 58023, *available at:* https://www.federalregister.gov/documents/2020/09/17/2020-20527/anti-money-laundering-program-effectiveness.

[36] Id., 58023.

[37] Id., 58025.

[38] Id., 58025.

The Blockchain Association fully supports and shares FinCEN's laudable goals of targeting money laundering, terrorism financing, and other illicit uses of digital assets. Because transparent blockchains create an immutable, public, and searchable record of all transactions in a given cryptocurrency, a recordkeeping requirement ultimately accomplishes the NPRM's objective of ensuring all relevant PII is retained and available for law enforcement purposes. Additionally, a recordkeeping requirement 1) avoids unnecessarily inundating FinCEN with a significant amount of highly sensitive "white noise," 2) effectively balances providing law enforcement useful information with respecting innocent users' right to privacy and security, thus addressing the core concerns raised in the over 7,000 comments FinCEN has received on this NPRM, and 3) better aligns with the goals of the AMLA and FinCEN's AML/CFT modernization effort. If FinCEN proceeds with an unnecessary reporting requirement, the Blockchain Association refers FinCEN to the comment letter submitted by Payward, Inc. and Circle Internet Financial for a description of the challenges and protocols FIs would need to address and develop to comply with a reporting requirement.

Sincerely,

Kristin Smith
Executive Director