CHAMBER OF DIGITAL COMMERCE

March 29, 2021
Via Federal E-Rulemaking Portal
Via email: frc@fincen.gov

Mr. Kenneth Blanco
Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
2070 Chain Bridge Road
Vienna, VA 22182

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

Dear Director Blanco:

The Chamber of Digital Commerce (the "Chamber") welcomes the opportunity to submit this supplemental letter for consideration by the Financial Crimes Enforcement Network ("FinCEN") with respect to the Notice of Proposed Rulemaking regarding "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "NPRM").[1]

FinCEN initially published the NPRM on December 23, 2020 and provided only 12 days to respond over the holiday period. The Chamber submitted a comment letter to this initial NPRM on January 4, 2021 in which, among other issues, we highlighted our significant concerns with respect to the truncated timetable given to respond to the NPRM as well as the need to address the erosion of traditional notions of financial privacy.[2] Since that

[1] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,840 (Dec. 23, 2020) (the "NPRM").
[2] Letter from Chamber of Digital Commerce to Financial Crimes Enforcement Network (Jan. 4, 2021), https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Chamber-of-Digital-Commerce_Comments_FINCEN-2020-0020-RIN-1506-AB47-Requirements-for-Certain-Transactions-Involving-Convertible-Virtual-Currency-or-Digital-Assets-c2.pdf.

time, on January 15, 2021, FinCEN published an additional notice in the Federal Register providing certain supplementary information and providing an additional 15 days to comment on certain aspects of the rule and 45 days to comment on other aspects (the "January 15 NPRM").[3] On January 28, 2021, FinCEN published a third notice providing a 60-day comment period for all aspects of the NPRM (the "January 28 NPRM").[4]

We are pleased that FinCEN has recognized the time provided under the NPRM and the January 15 NPRM was inadequate and has reopened the comment period. Given the complex nature of FinCEN's proposal, which would mark a dramatic shift from its current approach toward digital assets and customer due diligence and transaction reporting broadly, and unduly subject digital assets to stricter requirements than those in place for dealings in fiat currency, it is critical that industry be given sufficient time to assess the proposal and for FinCEN to engage proactively with industry to ensure that any final rule is both effective in combatting illicit finance and also reasonably implementable for industry. *Indeed, the recently passed Anti-Money Laundering Act of 2020 ("AMLA") mandates that FinCEN undertake a year-long, detailed study of existing currency transaction report ("CTR") and suspicious activity report ("SAR") requirements.*[5] As noted in our prior letter, the Chamber believes the proposed rule, as currently constructed, would hinder the important goal of countering illicit finance and present significant compliance challenges for industry that may be impossible to meet without engaging in substantial derisking and/or overreporting, and would compete with the AMLA-directed study of CTR and SAR requirements, a result that is contrary to the approach set out in the AMLA.[6]

This supplemental letter is provided in response to the January 28 NPRM and provides additional comments, suggestions, and concerns regarding this rulemaking process, which the Chamber was not able to address in its prior letter given the very condensed timeframe originally provided, as well as reactions to the supplementary information contained in the January 15 NPRM and comments on the recently passed AMLA implicating this rulemaking process. It also provides suggestions for amending the proposed rule to enhance its effectiveness in combatting illicit finance and reduce unnecessary burden on industry. More specifically, the Chamber supports a

[3] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86. Fed. Reg. 3897 (Jan. 15, 2021) (the "January 15 NPRM").
[4] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 7352 (Jan. 28, 2021) (the "January 28 NPRM").
[5] National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, H.R. 6395, 116th Cong. § 6204 (2021) (hereinafter "NDAA").
[6] The AMLA also directs Treasury to review "the most appropriate ways to promote financial inclusion and address the adverse consequences of financial institutions de-risking." *Id.* at § 6204.

recordkeeping requirement for transactions above $3,000, but believes such a requirement should be limited only to customer information (not counterparty information) and that industry should be given at least 180 days to allow adequate time to build compliance programs after issuance of a final rule. A reporting requirement should only be considered after FinCEN has completed the statutorily mandated studies, noted above.

We wish to highlight that the information contained below is intended to supplement the Chamber's prior letter and is not intended to replace or supersede that letter. Therefore, the fact that a given point addressed in the prior letter is not addressed in this letter should not be taken as an indication that the Chamber no longer holds that view, but only that the Chamber believes the matter was adequately addressed in its prior correspondence.

The Chamber looks forward to reviewing FinCEN's responses to the points raised in both of its submissions.

I. Introduction

The Chamber is the world's largest blockchain trade association. Our mission is to promote the acceptance and use of digital assets and blockchain technology, and we are supported by a diverse membership that represents the blockchain industry globally. Through education, advocacy, and close coordination with policymakers, regulatory agencies, and industry across various jurisdictions, our goal is to develop a pro-growth legal environment that fosters innovation, job creation, and investment. We represent the world's leading innovators, operators, and investors in the blockchain ecosystem, including leading edge startups, software companies, global IT consultancies, financial institutions, insurance companies, law firms, and investment firms. Consequently, the Chamber and its members have a significant interest in blockchain and distributed ledger technology and the impact of the NPRM, the January 15 NPRM, and the January 28 NPRM.

The Chamber and its members support FinCEN's important goals of combatting money laundering, terrorist financing, and other illicit acts. Detecting and preventing bad actors from utilizing blockchain and distributed ledger technology is both the right thing to do and essential to the long-term growth and success of the industry. This commitment can be seen across the industry and our member base. For example, Chamber member blockchain analytics and compliance firms such as Chainalysis, Elliptic, CipherTrace, Netki, TRM Labs, and others have developed cutting edge compliance tools that provide insight and analysis into transactions beyond what is available in the traditional fiat world.

Similarly, the Chamber itself is a co-founder of the Blockchain Alliance[7] and a co-lead in the Joint Working Group on interVASP Messaging Standards to aid with global implementation of the funds travel rule through its travel rule standard, IVMS 101.[8]

Notwithstanding its broad support for the Treasury Department's goals, the Chamber reiterates its serious concerns with respect to the NPRM. As noted in our prior letter, our concerns can be largely categorized in four broad buckets: (1) a misalignment between the purported goal of the rule and the rule's actual language and effect, (2) a severely understated estimation of the compliance burden placed on industry, (3) the likelihood the rule will undermine the important efforts of FinCEN to combat illegal use of cryptocurrencies by reducing the amount of actionable information reported and increasing the amount of unhelpful information reported, and (4) the likelihood that the rule will exacerbate existing privacy and cybersecurity considerations, and lead to a dramatic intrusion of government into the daily financial lives of Americans by providing Treasury visibility into nearly every blockchain transaction - past, present, and future - undertaken by banks' and money services businesses' ("MSBs") customers and the counterparties of those customers.

As discussed in our prior letter, we believe it is critical to note that self-hosted wallets play an important role in the digital asset ecosystem and, therefore, assertions that such wallets are inherently suspicious are unfounded.[9] Self-hosted wallets are no different than the wallet in a consumer's handbag or pocket: they help consumers hold different tools and assets that are used in the digital world, just like a wallet holds a consumer's cash, credit cards, or driver's license and allows that consumer to spend cash whether at the coffee shop, the hardware store, or an online retailer. Indeed, self-hosted wallets can similarly be used for more than just convertible virtual currency ("CVC"), they can also be used to store a consumer's driver's license, professional degrees or licenses, and other non-currency related items, to provide just a couple of examples. Self-hosted wallets are also critical to the development of future innovations in the blockchain ecosystem, including efforts to create and spur the adoption of central bank digital currencies, currently under study by a number of central banks around the world, including the Federal Reserve.

[7] Blockchain Alliance, https://www.blockchainalliance.org (last visited Jan. 4, 2020).
[8] interVASP Messaging Standard 101, https://intervasp.org/ (last visited Jan. 4, 2020).
[9] While FinCEN uses the term "unhosted" wallets in the preamble to the NPRM, that term is not defined nor does it appear in the actual text of the proposed rule. The Chamber believes that "self-hosted" more accurately describes the wallets at issue and, therefore, uses that term throughout.

Finally, the regulatory justifications for the proposed rule are likely to be found arbitrary and capricious. The NPRM describes its purposes as modestly extending existing reporting requirements for fiat currency transactions to CVC.[10] But in many respects, the NPRM and its successors create entirely new regulatory requirements unique to digital assets. This is especially true for the counterparty reporting and recordkeeping requirements, which have no analog in existing FinCEN regulations. Thus, the proposed rule cannot be justified on the basis of creating parity with fiat currency transactions. Nor does the NPRM's justification for extending the reporting and recordkeeping requirements account for the substantial likelihood that many regulated parties would forbid transactions with self-hosted wallets in cases in which they lack the ability to collect counterparty information or to assess the accuracy of such information. The NPRM wholly fails to grapple with both this derisking risk and the significant societal costs associated with derisking. FinCEN cannot justify what may turn out to be a *de facto* ban on many covered transactions on the grounds that the rule is a modest extension of existing reporting and recordkeeping obligations to digital assets.

II. Anti-Money Laundering Act of 2020

After publication of the NPRM, the National Defense Authorization Act for Fiscal Year 2021 ("NDAA"), which includes the AMLA, was enacted on January 1, 2021.[11] The January 15 NPRM cites the AMLA as providing additional statutory authority for the proposed rule. However, it ignores other relevant provisions of the AMLA impacting this process. Specifically, Section 6204 directs the Treasury Department, in conjunction with other federal and state authorities, to undertake a review of existing CTR and SAR requirements and to "propose changes to those reports to reduce any unnecessarily burdensome regulatory requirements and ensure that the information provided fulfills the purposes described in" the Bank Secrecy Act ("BSA"). Among other requirements, the review must consider:

- *the categories, types, and characteristics of suspicious activity reports and 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; and*

[10] *See e.g.*, NPRM at 83841, describing the requirements as "similar to the existing currency transaction reporting requirement."
[11] NDAA, Pub. L. No. 116-283.

- *whether the process for the electronic submission of reports could be improved for both financial institutions and law enforcement agencies, including by allowing greater integration between financial institution systems and the electronic filing system to allow for automatic population of report fields and the automatic submission of transaction data for suspicious transactions, without bypassing the obligation of each reporting financial institution to assess the specific risk of the transactions reported.*[12]

Therefore, Congress is clearly concerned that existing CTR and SAR reporting requirements are placing an undue burden on industry and producing significant volumes of unhelpful information for law enforcement.

Similarly, Section 6205 of the AMLA directs the Treasury Department, in conjunction with federal and state partners, to "review and determine whether the dollar thresholds, including aggregate thresholds" under the CTR and SAR rules "should be adjusted." Among other factors, the review should consider "the costs likely to be incurred or saved by financial institutions from any adjustment to the thresholds."[13] Thus, Congress is again making clear that the current CTR and SAR rules do not strike an appropriate balance between providing useful information to law enforcement and overly burdening industry.

It is also notable that Congress gave the Treasury Department a year to complete these reviews, reflecting the complexity of the issues and the importance of getting any regulatory changes right.

Given Congress's directive that the Treasury Department conduct an in-depth review of the CTR and SAR requirements, it makes no sense to proceed with a rulemaking that imposes additional reporting requirements prior to completion of that review; particularly when many of the issues identified by the Chamber and other commenters in response to the NPRM are precisely the same issues that Congress is expressing concern about in the AMLA. FinCEN should complete those reviews before adding new reporting requirements and forms, rather than release a rule that will be directly impacted by the results of the reviews — reviews which might result in material changes to or wholesale revocation of these requirements.

[12] *Id.* at Section 6204.
[13] *Id.* at Section 6205.

III. Comments on Additional Information Provided in the January 15 NPRM

In addition to providing additional time to comment, the January 15 NPRM provided additional detail on a number of important points.

a. Value Transaction Reports

The NPRM proposed to create a reporting requirement for transactions in CVC and legal tender digital assets ("LTDA") over $10,000 involving a self-hosted wallet. However, as noted by several commenters including the Chamber, the NPRM did not provide a draft of such form and instead stated, "Such report shall include, in a form prescribed by the Secretary, the name and address of each counterparty, and such other information as the Secretary may require."[14] The lack of specificity regarding the information to be reported made it impossible to comment on the feasibility or advisability of preparing and filing such reports.

The January 15 NPRM provided some additional detail by calling the form a "Value Transaction Report" and stating it would be similar to the currently existing CTR and include "information commonly associated with CVC and LTDA transactions."[15] It goes on to provide examples of fields, including:

a) *The CVC or LTDA type used in the transaction;*
b) *The transaction amount;*
c) *The assessed transaction value (in U.S. dollars);*
d) *The date and time of the transaction;*
e) *The transaction hash;*
f) *CVC or LTDA addresses involved in the transaction, and if they are hosted or unhosted;*
g) *The name and physical address of each counterparty to the transaction of the financial institution's customer; and*
h) *Other information readily available to the bank or MSB, which aids in identifying the specific reported transaction(s), the means by which it was conducted, and the parties involved.*

[14] NPRM at 38360.
[15] January 15 NPRM at 3898.

While this list is helpful, it leaves open many questions. Further, because the list is merely illustrative and the NPRM provides the Secretary considerable discretion in creating the form, it remains difficult to comment with certainty on the Value Transaction Report.

With respect to the specific examples cited in the January 15 NPRM, the Chamber is particularly concerned with examples (e), (f), and (g). First, providing the transaction hash means that FinCEN will have the wallet address of any MSBs' or banks' customers and counterparties (who may not be customers of those financial institutions) involved in a Value Transaction Report. By reviewing the transaction history of the wallet address associated with such persons, FinCEN can see all transactions such persons have ever made or will ever make using that wallet. Therefore, provision of the transaction hash in combination with the name and physical address of all counterparties inherently converts what should be a transaction-specific reporting requirement into a broad account reporting requirement with no temporal limitation. This raises a number of critical privacy and data security questions, which are discussed in further detail in our prior letter.

Moreover, almost all of the information requested in the draft Value Transaction Report is generally available from public sources. We question why this report is required at all, particularly in light of the AMLA's instruction to evaluate the necessity and utility of existing CTRs. The only pieces of information not generally available from public sources are the name and physical address *connected to* the other delineated information. Connecting this information, and then transmitting it to FinCEN, creates extraordinary financial privacy concerns, as well as an expansion of the way Treasury currently contemplates currency transaction and suspicious activity reporting obligations – on a transaction basis rather than an entire customer transaction history basis. It is the combination and automatic reporting to the government of this information that creates the extraordinary expansion of oversight of otherwise benign activity.

Second, as described in the Chamber's prior letter, there may be instances in which it will not be possible for members of industry to tell if a wallet is hosted or self-hosted. This uncertainty will cause many MSBs and banks to significantly overreport transactions by treating hosted wallets as self-hosted where a precise determination cannot be made, inevitably leading MSBs and banks to inadvertently provide misinformation in Value Transactions Reports.

In addition, FinCEN has previously issued guidance regarding hosted and self-hosted wallets, which the Chamber assumes should be used in making such determinations. However, any final rule should provide clear definitions of those terms or explicitly reference FinCEN's existing guidance on such terms. Furthermore, and as noted in our

prior letter, the preamble to the NPRM states that MSBs and banks must have a "reasonable basis" for determining that a wallet is hosted, but such a "reasonable basis" standard does not appear in the text of the actual proposed rule.

Third, the Chamber's prior letter describes in detail the difficulties MSBs and banks may have in obtaining counterparty information and the fact that institutions will likely need to rely on their customers to provide such information. As noted, the Chamber believes that, if implemented, the NPRM should explicitly permit banks and MSBs to obtain counterparty information from their customer and provide a safe harbor to rely on such information for banks and MSBs that do so.

In addition to the specific concerns with regard to examples (e), (f), and (g), we note that example (h) is simply too ambiguous for the Chamber to provide meaningful comment. FinCEN should clarify what is meant by this example so that industry can more accurately understand the information it would be expected to provide.

Finally, the Chamber wishes to thank FinCEN for clarifying that Value Transaction Reports would be filed through the existing BSA E-filing system and that batch reporting would be permitted.[16] As noted in our prior letter, given the anticipated volume of reportable transactions many of our members would handle, we believe permitting batch reporting through the E-filing system is essential.

b. Appropriate Length of Time to Comply

The January 15 NPRM states that requirements contained in the NPRM with respect to reporting, with the exception of reporting counterparty information (if adopted), would take effect 30 days after publication of a final rule. The reporting of counterparty information would take effect 60 days after publication of a final rule. The notice also states that the recordkeeping requirements would be effective 60 days after publication of the final rule. The January 28 NPRM makes no reference to these delayed effective dates.

While the Chamber believes a delayed effective date is clearly necessary, we believe the 30- and 60-day periods contained in the January 15 NPRM are plainly inadequate. As we described in our prior letter, complying with the requirements outlined in the NPRM will necessitate an investment of significant time and resources, including hiring additional compliance staff, revising policies and procedures, onboarding new vendors or service providers, and building new technology solutions. Setting aside the significant cost of

[16] January 15 NPRM at 3898.

such measures, MSBs and banks cannot be expected to accomplish such tasks in 30 or 60 days.

In reality, such measures are likely to take several months to implement. That is based not only on member estimates with respect to this proposed rule, but real-world experience in adjusting to significant regulatory changes in other jurisdictions. Based on member experience, a typical process for implementing such a significant change is as follows:

1. Become familiar with the technical solution of an external vendor and assess its strength in a demo environment (~2-3 weeks at minimum);
2. Perform a security review of the technology vendor (plus complete legal paperwork / the procurement process, as applicable) (4 weeks or more, although this can be done concurrently with the following steps);
3. Perform technical integration of the external solution via APIs (~2 weeks);
4. Implement changes to current customer flows (*e.g.*, collection of counterparty info), in addition to changes in the platform backend (*e.g.*, aggregation of transactions triggering reporting requirements) (~4-6 weeks);
5. Internal testing of the compliance solution with the institution's own blockchain transaction flow (~2-4 weeks); and
6. Building compliance processes and training compliance teams to monitor transactions and identify different scenarios when manual intervention is necessary (~4-6 weeks).

Notably, this timeline assumes that an institution is already familiar with the new regulatory requirements and with potential technology vendors, such that it can begin this process immediately upon issuance of a final rule. It also assumes that appropriate technology solutions exist, such that they can be immediately implemented. While a number of companies are working on rolling out technology solutions, progress varies across companies. It is likely that when a final rule is issued only a few vendors will have a technology solution readily available, which could lead to a backlog for those vendors as they seek to keep up with demand.

Finally, for many companies, it may be necessary to hire new personnel to assist in complying with the final rule. Members report that hiring qualified compliance personnel and training such personnel on the company's policies and procedures can take 1-2 months.

Given the above, we believe the effective date should be no earlier than 180 days after publication of a final rule.

IV. Responses to Additional Questions Posed in the NPRM

As noted in our prior letter, it was simply not feasible for the Chamber to respond to all of the NPRM questions it wished to address given the limited window provided for industry to comment. Therefore, we take this opportunity to address a number of the questions we were not able to specifically address in our prior letter.

a. Should FinCEN add additional jurisdictions to the Foreign Jurisdictions List or remove jurisdictions currently on that list? Are there any particular considerations FinCEN should take into account when adding or removing jurisdictions?

As noted in our prior letter, we believe that creation of the Foreign Jurisdictions List is unnecessary and duplicative. The NPRM states that the list would initially include Iran, North Korea, and Burma. Iran and North Korea are already subject to comprehensive embargoes imposed by the Office of Foreign Assets Control ("OFAC"), meaning nearly all transactions involving the two countries are prohibited. Burma is included on the Financial Action Task Force's ("FATF") so-called "grey list" as a jurisdiction with strategic deficiencies and therefore may already be treated as higher risk by banks and MSBs.[17] All three jurisdictions are also subject to special measures pursuant to Section 311 of the USA PATRIOT ACT (Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern).[18] Therefore, the inclusion of an additional FinCEN list would add little or no value as compared to existing requirements and controls applicable to all financial institutions.

If FinCEN believes that creation of a Foreign Jurisdictions List is necessary, we believe it should provide clear criteria by which the agency will determine whether to include or remove a jurisdiction. One such approach would simply be to reference an existing list such as jurisdictions subject to special measures pursuant to Section 311 or the FATF's list of high-risk jurisdictions subject to a call for action (the so-called "black list"). Indeed, the NPRM states that the original three jurisdictions were selected because they were previously designated as jurisdictions of primary money laundering concern pursuant to

[17] On February 11, 2021, President Biden issued an Executive Order entitled *Executive Order on Blocking Property with Respect to the Situation in Burma* authorizing the imposition of targeted sanctions on certain Burmese individuals and entities. Executive Order No. 14014, 86 Fed. Reg. 9429 (Feb. 10, 2021). While these sanctions are significant, they do not amount to a comprehensive embargo of the type currently in place against Iran and North Korea.

[18] 31 U.S.C. § 5318A.

Section 311.[19] Ultimately, though, we see no reason to deviate from that initial approach by creating a new, separate list.

b. Could the verification requirements be adjusted to enhance the benefits to law enforcement without a significant change to the costs to banks and MSBs, or to reduce the costs to banks and MSBs without a significant change in the benefit to law enforcement?

The Chamber is a strong supporter of various digital ID systems being developed and implemented around the world, which promise to allow faster, more secure, and more accurate identification of users. Many of these systems rely on blockchain technology, making them of even greater interest to our members. We believe that any final rule should be flexible enough to allow for innovative approaches to customer identification and verification, including the use of emerging digital ID systems. An overly prescriptive identification and verification requirement will stifle innovation of these important technologies and place U.S. financial institutions at a competitive disadvantage versus many of their overseas counterparts.

The Chamber believes that any final rule should specifically permit use of digital identity systems and create a regulatory sandbox that encourages banks and MSBs to test or pilot emerging digital ID systems. Such provisions should also be harmonized with ongoing efforts from national and international standards-setting bodies, including the FATF's recently released Guidance on Digital ID.[20]

c. Is it necessary for the anti-structuring prohibition to be extended to the proposed CVC/LTDA transaction reporting requirement?

As noted in our prior letter, the Chamber has considerable concerns regarding the aggregation requirement contained in the NPRM. Specifically, MSBs and banks will need to implement new technology solutions to aggregate transactions, including transactions conducted in different CVCs, and to do so on a continuous, rolling 24-hour basis. The aggregation requirement as drafted also contains a number of ambiguities, including: (1) if value in and value out transactions should be aggregated together or if they should be calculated separately for purposes of the $10,000 threshold, and (2) whether exempt

[19] NPRM at 83843.
[20] Financial Action Task Force, *Guidance on Digital ID* (Mar. 2020), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

transactions should be included when aggregating transactions.[21] While preventing customers from circumventing FinCEN reporting and recordkeeping obligations is critically important, the Chamber believes that having an appropriately tailored and clear aggregation requirement is an essential first step before any anti-structuring measures should be imposed.

d. Is it reasonable to require that records be retained in electronic form? Are the retrievability criteria reasonable?

The Chamber believes that a requirement for records to be stored in electronic format is appropriate. Nearly all of our members store records in electronic form and find such storage to be more secure, efficient, and effective than storage of records in hardcopy format.

With respect to retrievability, the Chambers believes that a requirement for records to be retrievable by customer name or account number is a reasonable requirement that generally comports with industry practices. Because we do not believe the proposed rule should be extended to counterparty information, we believe a requirement that counterparty information be searchable by name should be stricken from any final rule.

V. Additional Detail on Matters Raised in Our Prior Letter

As noted in our prior letter, a number of topics we addressed in cursory fashion given the limited time to respond. We have provided additional detail on a number of these topics below.

a. Decentralized Finance, Decentralized Applications, and Smart Contracts

As stated in our prior letter, it is unclear whether the recordkeeping and reporting provisions of the NPRM would be triggered when MSBs and banks engage in certain activity involving decentralized finance ("DeFi") projects, such as decentralized applications ("DApps") or smart contracts. Indeed, in many situations the provisions outlined in the NPRM simply do not correspond to the reality of the financial transactions in DeFi projects. Consider two examples cited in our prior letter:

[21] The Chamber believes that exempt transactions should not be included and that FinCEN likely did not intend for them to be included. However, the NPRM's silence on this issue has the potential to create confusion and lead industry to take an inconsistent approach. We therefore request that any final rule explicitly state that exempt transactions should not be included when aggregating transactions.

- funds sent or received from a non-custodial smart contract, particularly where the contract has no direct owner or is owned by hundreds or thousands of governance token holders; and
- smart contract transactions that involve multiple persons in the transaction chain, one or more of whom may be unknown to the original transferor, such as in the case of trade finance and smart contracts intended to mimic letters of credit or similar instruments.

If DeFi, DApps, and smart contracts are not specifically addressed in any final rule, we fear that many MSBs and banks will stop integrating these types of protocols into their product offerings, which would scuttle their opportunity to create efficiencies in financial markets, eviscerate their ability to compete in a rapidly evolving industry, and harm consumers whose access to such projects would be jettisoned.

The Chamber believes the NPRM simply does not reflect the realities of many DeFi projects, and that attempting to shoehorn DeFi into a rule intended for other types of non-decentralized blockchain products would present a variety of serious complications for DeFi projects, consumers, and FinCEN. Indeed, based on the preamble to the NPRM, it appears that FinCEN did not consider DeFi before issuing the proposed rule. Given that the proposed rule does not appear intended to apply to DeFi and that attempting to graft it onto DeFi projects would be nearly impossible, the Chamber believes the most prudent course would be to specifically exempt DeFi from the rule's scope.

Before FinCEN addresses DeFi in any rulemaking, however, we believe the agency should publish revised guidance that provides industry with greater clarity on how the agency understands terms such as DApps and decentralized exchanges, both of which are addressed in FinCEN's 2019 CVC guidance but are not defined in sufficient detail for industry to have clarity on whether a given project falls within the meaning of those terms for purposes of this rulemaking. Resolving these basic definitional questions is an essential first step before any DeFi projects are addressed in a rulemaking.

b. Layer 2 Protocols

Our prior letter highlighted that the NPRM does not address how banks and MSBs should handle transactions involving "layer 2" solutions such as the Lightning Network. The Lighting Network uses off-chain micropayment channels that allow counterparties to engage in multiple off-chain transactions, which are recorded to the blockchain when the counterparties open and close a channel.

Such a model raises a number of questions including, among others: what constitutes a "transaction," how to determine the time that a transaction "occurred," and how to handle off chain transfers where no transaction hash is typically available.

We believe the most appropriate method for handling layer 2 protocols is to require recordkeeping and reporting only when a channel is closed. If FinCEN believes that more regular reporting is necessary it should provide specific guidance on the above questions and how to handle data fields such as "transaction hash," which does not exist until the channel is closed.

c. Implications for LTDA

We believe inclusion of LTDA in any final rule would be premature given that LTDA are currently not widely used anywhere in the world and, therefore, it is impossible to fully understand the implications for extension of this rule to LTDA. While a number of jurisdictions, including the United States, have announced they are studying LTDA or conducting pilot programs, no jurisdiction has issued a widely utilized LTDA.[22] Therefore, no significant data exists to assess how such assets are likely to be used, who is likely to use them, how users would obtain such assets in the first instance, and many other critical questions.[23] As such, it is nearly impossible for industry to provide meaningful comments, and the potential for creating unintended consequences is significant.

From the information that is available, we believe FinCEN should not include LTDA in the proposed rule. The NPRM defines LTDA broadly to include "any type of digital asset issued by the United States or any other country that is designated as legal tender by the issuing country and accepted as a medium of exchange in the country of issuance."[24] Such a definition would seemingly capture a wide array of assets, including, for example,

---

[22] *See, e.g.,* Nikhilesh De, *The Federal Reserve Is Experimenting With a Digital Dollar*, Coin Desk (Aug. 13, 2020), https://www.coindesk.com/the-federal-reserve-is-experimenting-with-a-digital-dollar; Jonathan Cheng, *China Rolls Out Pilot Test of Digital Currency*, The Wall Street Journal (Apr. 20, 2020), https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339. Venezuela has issued an LTDA known as the petro; however, transactions or dealings in the petro by U.S. persons or within the United States are prohibited pursuant to Executive Order No. 13827, 83 Fed. Reg. 12,469 (Mar. 19, 2018).

[23] The Chamber addresses some of the functional and policy considerations of a U.S.-issued LTDA in its letter to the Conveners of the Digital Dollar Project. Letter from the Chamber of Digital Commerce to the Conveners of the Digital Dollar Project, *The Digital Dollar Project: Exploring a US CBDC* (Oct. 2, 2020), https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2020/10/Chamber-of-Digital-Commerce-Digital-Dollar-Project-White-Paper-Response-Letter.pdf.

[24] NPRM at 83860.

a digital dollar. Inclusion of a digital dollar within the scope of this rule would serve to exacerbate the already significant privacy concerns raised by the Chamber in its prior letter.[25] As noted, provision of a transaction hash in combination with the name and physical address to FinCEN will provide the government with insight into every transaction conducted by a given wallet – past, present, or future. While this presents significant privacy concerns for users of CVC, such users at least have the option to use an alternative payment mechanism, if so inclined. If the United States were to launch a digital dollar to which this rule extended, users may have no choice but for the government to have nearly complete visibility into all of their transactions over the course of their lifetime. This would be a shocking result, but is a potential consequence of extending this rule to LTDA.

FinCEN should continue to monitor the development of such assets and, if appropriate, solicit input from industry at a later point in time when industry would be able to provide more meaningful comments and the consequences, including any unintended consequences, of extending such a rule to LTDA could be ascertained with a greater degree of certainty. There is simply no reason to act on LTDA at the present point in time without any meaningful engagement in this type of asset.

d. Financial Inclusion

A desire for financial inclusion has long been at the center of the blockchain industry, and promoting equity in financial services is a core goal of many Chamber members. The Chamber is encouraged that Secretary Yellen seems to share this important goal. As she recently told the Senate Finance Committee, the "issues of diversity, inclusion and racial equity are incredibly important, particularly at this moment in history when the pandemic has taken an unbelievable and disproportionate toll on low-income workers and especially people of color."[26] Secretary Yellen also noted the first meeting she took after the announcement of her nomination was with "representatives of racial and economic

[25] These issues were also addressed by the Chamber in its letter to the Digital Dollar Project, in which we note "Besides recognizing the important role the prohibition against unreasonable searches and seizures the U.S. Constitution's Fourth Amendment will play in any discussion of privacy, when it comes to a U.S. CBDC, our Members believe that additional work will need to be done on this front before a digital dollar will be ready for widespread use. Any potential U.S. CBDC should carefully balance law enforcement and compliance objectives with user privacy." Letter from the Chamber of Digital Commerce to the Conveners of the Digital Dollar Project, *The Digital Dollar Project: Exploring a US CBDC* (Oct. 2, 2020), https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2020/10/Chamber-of-Digital-Commerce-Digital-Dollar-Project-White-Paper-Response-Letter.pdf.

[26] FINANCE COMMITTEE QUESTIONS FOR THE RECORD: Hearing on the Nomination of Dr. Janet Yellen Before the S. Comm. On Fin., 117th Cong. 34 (2021) (Responses by Dr. Yellen).

justice groups to hear directly from them what their needs are."[27] The Chamber was similarly pleased to see Congress require the Treasury Department to review "the most appropriate ways to promote financial inclusion and address the adverse consequences of financial institutions de-risking" in the recently passed AMLA.[28] While we encourage Secretary Yellen and Congress to prioritize this important issue, we worry the NPRM will have the opposite effect by reducing financial inclusion and making financial services harder to access for many Americans.

Too many Americans, particularly those from communities of color, as well as lower-income and immigrant communities, lack access to basic financial services. A 2019 report from the Federal Deposit Insurance Corporation ("FDIC") finds that 5.4% of all American households are completely unbanked, meaning that no one in the household had a checking or savings account at a bank or credit union.[29] Among Black households that number was even higher at 13.8% and among Hispanic households it was 12.2%.[30] Survey participants cited a number of factors as a reason for not having a bank account, including not having enough money to meet minimum balance requirements (48.9%), a lack of trust in banks (36.3%), a desire to retain privacy (36.0%), high account fees (34.2%), unpredictable account fees (31.3%), personal identification, credit, or former bank account problems (20.5%), banks not offering needed products and services (19.6%), inconvenient bank locations (14.1%), and inconvenient bank hours (13.0%), among others.[31] The problem is even worse globally with an estimated 1.7 billion adults unbanked according to the World Bank.[32] Lack of access to traditional bank accounts can have a variety of negative consequences, including difficulty accessing credit, difficultly obtaining a loan, and difficultly getting paid and making payments, to name but a few.

The blockchain industry has long been a leader in expanding access to financial services in the United States and around the world. Self-hosted wallets play a critical role in that expansion as they allow users to send and receive funds with just a smartphone, which in turn opens an array of additional financial services. The Chamber believes that blockchain and, in particular, self-hosted wallets, can be a critical tool in expanding

---

[27] *Id.*
[28] NDAA at § 6204.
[29] Federal Deposit Insurance Corp., How America Banks: Household Use of Banking and Financial Services (2020), https://www.fdic.gov/analysis/household-survey/2019execsum.pdf at 1.
[30] *Id.* at 2.
[31] *Id.* at 3.
[32] The World Bank, The Global Findex Database (2017), https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf at pg. 35.

access to financial services and reducing poverty at home and abroad, while maintaining a public ledger of the transfers. Indeed, blockchain technology has the potential to solve or ameliorate many of the concerns cited by unbanked persons in the FDIC study, including high or unpredictable fees, a desire to retain privacy, lack of trust in traditional financial institutions, and inconvenient bank locations and hours. Self-hosted wallets put the consumer in control, enabling them to take advantage of transactions and financial services that have been denied to them in the traditional fiat context.

Given the critical role that blockchain and self-hosted wallets can play in promoting financial inclusion, the Chamber believes measures that disincentivize or stigmatize use of self-hosted wallets should be avoided. For the reasons discussed throughout this letter and our prior letter, we believe the NPRM may lead to significant derisking by MSBs and banks, reducing the ability of self-hosted wallet holders to access or be involved in blockchain-related financial services.

e. Risk-Based Approach to CVCs

As drafted, the NPRM treats all assets meeting the definition of CVC the same. The Chamber believes this is the correct approach and encourages FinCEN to adopt this approach in any final rule. While different CVCs vary in terms of their functionality, ease of use, privacy protections, and other features, the Chamber believes that attempting to create rules for various sub-classes of CVC, such as anonymity enhanced cryptocurrencies or "AECs," would inevitably lead to confusion and be extremely difficult to apply in practice, given the number of different CVCs currently available and the rapid pace of development of CVCs with new features or new combinations of features.

Instead, banks and MSBs should take a risk-based approached where they consider the specific risks posed by each CVC in which they deal and determine what, if any, additional mitigation measures should be undertaken with respect to a given CVC. FinCEN frequently advocates such an approach when interacting with industry and the Chamber is pleased to see that approach appears to be incorporated into the NPRM.

f. Fourth Amendment Considerations

Whether blockchain users have a reasonable expectation of privacy in blockchain data and information held by banks and MSBs is an underdeveloped area of privacy law.

Indeed, the Fifth Circuit is the only appellate court to have addressed this issue in *United States v. Gratkowski*.[33]

As a general matter, individuals have Fourth Amendment protection from unreasonable searches when they have a "reasonable expectation of privacy" in the items to be searched.[34] For records held at financial institutions, the Supreme Court has generally relied upon the third-party doctrine, which holds that a person "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[35] This includes the Supreme Court's seminal decision in *U.S. v. Miller* holding a bank depositor did not have a privacy interest in financial records maintained by the bank.[36] However, in recent years, the Supreme Court has indicated there are limits to the third-party doctrine, finding in *Carpenter v. U.S.* a privacy interest in cell site location data, given the intimate nature of the information and lack of any true intent to share such information on the part of cell phone users.[37]

While *Gratkowski* held that a *customer* of a CVC exchange did not have a reasonable expectation of privacy in public Bitcoin blockchain records or information held by an exchange, we believe that the principles articulated by *Gratkowski*, and the Supreme Court cases on which it relies, clearly demonstrate that the NPRM does violate the Fourth Amendment, at least with respect to *counterparty* information.

In finding that Gratkowski did not have a privacy interest in information held by an exchange, the court analogized to the Supreme Court's ruling in *Miller* regarding bank records. In drawing the analogy, the *Gratkowski* court states "the nature of the information and the voluntariness of the exposure weigh heavily against finding a privacy interest" in the CVC exchange's records.[38] It also distinguishes from the Supreme Court's ruling in *Carpenter* by noting the exchange records are "limited" and do not provide "an intimate window into a person's life" and that the decision to use the exchange was an "affirmative act on part of the user."[39]

However, neither of the two factors relied upon by the *Gratkowski* court are present with respect to the NPRM. First, the information provided would not be limited and would in fact provide an extremely intimate window into a person's life. As described above, this

[33] *U.S. v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020).
[34] *U.S. v. Jones*, 565 U.S. 400, 406 (2012).
[35] *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).
[36] *U.S. v. Miller,* 425 U.S. 435 (1976).
[37] *Carpenter v. U.S.,* 138 S. Ct. 2206 (2018).
[38] *Gratkowski*, 964 F.3d at 312.
[39] *Id.* (quoting *Carpenter*, 138 S. Ct. at 2210).

is because reporting of transaction hashes and associated names of customers and counterparties will allow FinCEN to develop a detailed map of blockchain address owners which, when combined with other information on the blockchain, would allow FinCEN to see every transaction undertaken by a customer or counterparty – past, present, or future. In essence, such persons would no longer have any privacy in their financial dealings involving blockchain (and potentially including a digital dollar or other LTDA). If that is not an intimate window into a person's life then nothing is.

Second, while customers may voluntarily choose to use the services provided by an exchange, counterparties do not. Indeed, counterparties may have no idea that their information has been provided to an exchange and subsequently reported to the government. As such, the reporting of counterparty information clearly cannot be considered voluntary or the result of an affirmative act on the part of the counterparty.

Finally, *Gratkowski* places considerable emphasis on the public nature of the Bitcoin blockchain in reaching its conclusions. The Chamber does not contest that certain Bitcoin blockchain information is inherently public (including wallet addresses and transaction amounts) and indeed promotes that fact for compliance purposes. However, a user's name and physical address are decidedly not included within such public information and it is this non-public information whose disclosure is violative of the Fourth Amendment. Further, we note that blockchains vary considerably in the type and amount of information that is publicly available, meaning analysis with respect to one blockchain is not necessarily applicable to another.

VI. Suggestions for Improving the NPRM

As noted above, FinCEN is about to undertake a review of existing CTR and SAR reporting requirements, as mandated by Congress in the recently passed AMLA. That review will consider essential questions regarding the existing requirements including whether the requirements are effectively providing law enforcement with useful information and whether the useful information that is derived is appropriately balanced against the burden placed on industry. Indeed, many of the questions Congress directs FinCEN to consider in the AMLA are the same questions that FinCEN posed to industry in the NPRM. Adding a new reporting requirement before that review is completed, and the findings can be shared with industry and incorporated into any new reporting requirement, makes little sense and cuts against the intent of Congress.

As a result, we believe that any final rule should be limited to recordkeeping requirements.[40] The Chamber believes that $3,000 is an appropriate level for the recordkeeping requirement. That is the same level that applies under FinCEN's so-called "travel rule."[41] Having a harmonized approach between the travel rule and any requirements imposed by this rulemaking process will help reduce the burden placed on industry and increase the effectiveness of banks' and MSBs' compliance programs. Travel rule compliance necessitates determining whether a given transaction involves a wallet held at another financial institution (typically another bank or MSB). Such a determination is essentially the inverse of that required under this NPRM (*i.e.*, whether a given transaction involves a self-hosted wallet). By having a harmonized threshold between the travel rule and this rule, banks and MSBs can have a single decision point, reducing unnecessary duplication of compliance measures and helping ensure a consistent approach is taken across an institution's compliance function.[42] A $3,000 threshold is also consistent with the approach FinCEN has taken in other contexts, including issuing or selling bank checks or drafts, cashier's checks, money orders and traveler's checks under 31 C.F.R. § 1010.415.

For the reasons noted above, we believe reporting on counterparty information is extremely problematic, violates the Fourth Amendment, and should not be included in this rulemaking.

While the Chamber does not believe that a reporting requirement is necessary or appropriate at this time, we note that the lack of a reporting requirement is unlikely to hamper FinCEN and law enforcement access to the collected information as the recorded information could be requested by the agency through a 314(a) request or similar tool. Such an approach makes sense in the blockchain context, as opposed to the fiat currency context, because so much information is already publicly available on most blockchains.

---

[40] As noted in our prior letter, such a recordkeeping requirement should not apply when a customer is moving funds between a bank or MSB and a self-hosted wallet owned by the customer. These types of transactions are clearly distinct from transactions that involve a third party and application of the rule's requirements to such transactions is unlikely to generate any new or useful information for FinCEN or law enforcement.

[41] An NPRM published on October 27, 2020 by FinCEN and the Board of Governors of the Federal Reserve System proposes to lower the applicable threshold for certain transactions. The Chamber previously submitted a comment letter opposing a lowering of the threshold, which is available at: https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2020/11/Chamber-of-Digital-Commerce-Response-to-FinCEN-Travel-Rule-NPRM-112520.pdf.

[42] The Chamber believes that both the travel rule and any requirements stemming from this rulemaking process should include within them a procedure to automatically adjust the applicable threshold on an annual basis, based on inflation. In the absence of a mechanism to adjust for inflation, the thresholds will continually apply to a greater and greater proportion of transactions, increasing the burden on industry without any justification.

In the fiat currency context, if no report is made to FinCEN, the agency would have no knowledge that a cash transaction over $10,000 occurred. The same is not true for blockchain transactions where FinCEN can easily track the movement of CVC between wallets. Indeed, for most blockchains, the only information called for in the NPRM that is not publicly available is the name and physical address of the wallet holder. If FinCEN identified a transaction over $10,000 of interest to the agency, it could simply issue a request to MSBs and banks and obtain any information such institutions had regarding those wallets. The Chamber notes that FinCEN has access to the same blockchain analytics tools used by industry and, therefore, could deploy such solutions to assist it in identifying transactions of potential interest.[43] Such an approach would significantly lessen the burden placed on industry, reduce the volume of unhelpful information being reported, and lessen the serious privacy concerns cited above.

Finally, we believe that any recordkeeping requirement should not include a requirement with respect to counterparty information. As noted above and in our prior letter, the inclusion of a counterparty requirement exceeds the requirements imposed on fiat currency transactions, would significantly increase the burden placed on industry, exacerbate the considerable privacy concerns already raised by this rulemaking, and place industry in the impossible position of being required to record information without a clear means to confirm its accuracy.[44] This is not to say that banks and MSBs would never collect counterparty information, but rather that they would have the ability to elect whether and at what threshold to collect such information using a risk-based approach.[45] This risk-based approach is in keeping with FinCEN's general approach toward BSA implementation, as well as that of international institutions such as the FATF.[46] Particularly given the diverse and rapidly evolving nature of the blockchain industry, it makes little sense to veer away from this traditional risk-based approach toward a one-size-fits-all model.

---

[43] While the availability and functionality of such tools varies depending upon the blockchain in question, analytics companies are continually updating and upgrading their offerings.

[44] If FinCEN were to require the collection of counterparty information above a certain threshold, it should make clear that banks and MSBs should be able to obtain counterparty information from their customers and should be permitted to rely on such information.

[45] Banks and MSBs may also take a variety of other risk-based measures with regard to counterparties such as subjecting the wallets to screening through analytics tools, cross-referencing the addresses against sanctions lists, or whitelisting certain addresses, such as when a customer can prove it owns a given self-hosted wallet.

[46] *See, e.g.*, FinCEN, Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (Apr. 26, 2005), https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf; Financial Action Task Force, FATF takes action to tackle de-risking (Oct. 23, 2015), https://www.fatfgafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html.

VIII. Timing with Respect to Travel Rule

On October 27, 2020, FinCEN issued a proposed rule with respect to the travel rule that would lower the threshold for travel rule compliance for certain transactions and purports to "clarify" the application of the rule with respect to CVC.[47] The Chamber requests that FinCEN not issue a final rule, or at a minimum not require compliance with that rule, until after FinCEN has issued a final rule with respect to the travel rule and that rule is implemented broadly across industry. Once travel rule solutions are broadly adopted across industry it may assist in identifying a significant amount of hosted wallets and thus lower the risk of misclassifying wallet addresses, and of collecting and sharing unnecessary or inaccurate information. Such a sequential implementation would also allow industry to apply technology solutions, newly developed processes, and lessons learned from the travel rule context to the self-hosted wallet context.

While such a sequential approach would lead to a somewhat longer timeframe with respect to finalization of the NPRM, it would still be significantly shorter than the timeframe for other recent, significant rulemakings. In particular, and as cited in our prior letter, the customer due diligence rulemaking process took approximately four years to complete, reflecting the agency's understanding that it was more important to get the rulemaking right than to do it quickly – an approach that should be brought to the current rulemaking as well.

IX. Conclusion

The Chamber appreciates the opportunity to comment on this important issue and appreciates that FinCEN reopened the comment period to allow industry a meaningful opportunity to participate in the rulemaking process.

Given the wide range of open questions, concerns, and suggestions raised in this letter, our prior letter, in comments submitted by other members of industry, and in fact even by Congress both by letter[48] and in legislation (the AMLA), we believe the appropriate path

---

[47] Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status, 85 Fed. Reg. 68,005 (Oct. 27, 2020), https://www.govinfo.gov/content/pkg/FR-2020-10-27/pdf/2020-23756.pdf. The Chamber previously submitted a comment letter in response to that proposed rule, available at: https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2020/11/Chamber-of-Digital-Commerce-Response-to-FinCEN-Travel-Rule-NPRM-112520.pdf.

[48] Letter from Members of Congress to Secretary of the Treasury Steven Mnuchin (Dec. 31, 2020), https://emmer.house.gov/_cache/files/8/a/8a474348-cf14-467d-8c1d-

forward would be for FinCEN to engage in public-private discourse to better understand where law enforcement currently has appropriate tools from publicly available information, how blockchain analytics firms are already creating advancements for law enforcement, how blockchain technology itself can help modernize our AML tools, and what might be an appropriate path ahead. Moving directly to a final rule without additional opportunity to better address these topics would risk creating a final rule that is unworkable, unhelpful to the important goals of FinCEN, or that produces significant unintended consequences. In any circumstance, issuance of a new notice should come after the Treasury Department has completed its review of current CTR and SAR rules, as required by Congress.

The Chamber shares FinCEN's important goals of combatting illicit finance and is committed to working cooperatively with the agency to help produce a rule that assists law enforcement while not unduly burdening industry.

Very truly yours,

Amy Davine Kim
Chief Policy Officer

cc: Jason Weinstein
Alan Cohn
Shannen Coffin
Evan Abrams
Steptoe & Johnson LLP

bdc9c221df0a/7A3776731990BD312FCCE841E096D82B.congressional-letter-to-treasury-123120done.pdf.