CHAMBER OF DIGITAL COMMERCE

November 25, 2020

Submitted via Email
Regs.comments@federalreserve.gov
frc@fincen.gov

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Policy Division
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Re: Federal Reserve Docket No. R–1726; RIN 7100–AF97;
FinCEN Docket Number FINCEN–2020–0002; RIN 1506–AB41

Dear Secretary Misback and Financial Crimes Enforcement Network Policy Division:

The Chamber of Digital Commerce (the "Chamber") welcomes the opportunity to submit this letter for consideration by the Board of Governors of the Federal Reserve System (the "Board") and the Financial Crimes Enforcement Network ("FinCEN") with respect to the Joint Notice of Proposed Rulemaking related to the "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" (the "NPRM").[1] The NPRM proposes changes to the Recordkeeping Rule, which requires bank and nonbank financial institutions to collect and retain information related to funds transfers and transmittals of funds in amounts of $3,000 or more, and the Travel Rule, requiring bank and nonbank financial institutions to transmit information on certain funds

[1] 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) (hereinafter, the "NPRM").

transfers and transmittals of funds to other bank or nonbank financial institutions participating in the transfer or transmittal.[2] (Collectively referred to as the "Rules").

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 financial institutions, leading edge startups, software companies, global IT consultancies, insurance companies, law firms, and investment firms. Consequently, the Chamber and its members have a significant interest in blockchain and distributed ledger technology ("DLT").

I. Executive Summary

In this letter, we provide the following perspectives:

- The United States is already at a competitive disadvantage with respect to its promotion of blockchain-related business. These companies are looking for other jurisdictions to conduct business – countries that have clear regulatory regimes and seek to promote responsible innovation. A rule that is *more* restrictive than international recommendations only serves to further that reality.

- We agree with the principle that the applicability of the Travel Rule was unclear previously and appreciate the NPRM's goal to clarify it. We do not believe that convertible virtual currency ("CVC") should be included in the definition of "money;" however, if FinCEN determines to move forward with this proposal, we suggest corrections to the definition.

- With respect to the reduction in threshold:

    - This is a substantial decrease in the threshold, one that impacts significant personnel and technological systems and, ultimately, cost. Thirty days is insufficient time to calculate the various implications of this adjustment and we request more time in which to consider it.

    - A 92% decrease in the recordkeeping threshold creates an exponential increase in compliance costs that reverberate throughout compliance systems beyond the initial widening in scope of the number of originators/beneficiaries. It also negatively impacts financial inclusion –

[2] Recordkeeping requirements for banks are set forth in 31 CFR 1020.410(a); for nonbanks at 31 CFR 1010.410(e); and the Travel Rule is set out at 31 CFR 1010.410(f).

we should encourage more participation within the regulated financial system, not less.

- We suggest maintaining the $3,000 threshold while this industry is building a globally viable system of transferring personally (and commercially) identifiable information that must be protected for privacy and cyber security purposes. At a time when countries are doing more to protect these concepts, this NPRM creates significant exposures that require careful attention.

- We request a safe harbor for U.S. financial institutions to exempt them from the requirement to transmit personal and commercial data to third parties until an operational system to protect them is in place. This "safe harbor" would be similar to exemptions provided by FinCEN when originally implementing the Travel Rule.

II. Introduction

Blockchains provide an unprecedented ability to track and trace transactions historically, both by token and by wallet/account. Chamber Members Chainalysis, Elliptic, CipherTrace, and others are offering compliance-oriented services for blockchain technology and helping governments and businesses (including financial institutions) to identify and mitigate risk and enable companies to alert law enforcement to potentially suspicious transactions. Unlike cross-border wire transfers, blockchains perfectly preserve the provenance of financial transactions and do not suffer from data integrity issues. Chamber Member Netki has created a compliance data communications channel solution to enable businesses to privately and securely exchange compliance and other metadata related to transactions, sanctions screening, and other regulatory requirements. Chamber Member FinClusive offers the assignment of unique identifiers ("FinCID") to all clients/subjects that come through its comprehensive KYC/KYB process and are engaged in transfers of value via blockchain-enabled and peer-to-peer systems, which enable counterparties to trace transactions to appropriate sender/receivers while also protecting essential personal identifying information ("PII") associated with those individuals and entities. Indeed, the ability to trace transactions back through time is a technological advancement that has already provided a boon to law enforcement in its efforts to detect and prosecute criminals.

Blockchains can enhance law enforcement efforts in other ways as well. For instance, with respect to Bank Secrecy Act ("BSA") and Office of Foreign Assets Control ("OFAC") compliance obligations, blockchain technology can support Know Your Customer ("KYC") management in ways that ensure that the characteristics of the customer, including beneficial ownership, are established and verified securely and efficiently. Further, blockchain-enabled KYC, customer due diligence ("CDD"), and transaction monitoring could be used to enhance the Section 314 information sharing process – both under Section 314(a) as well as 314(b) (communications between institutions and law enforcement as well as among institutions, respectively) to ensure

that data shared is accurate and comprehensive. It could also strengthen (real time) auditability of financial transactions between counterparties; facilitate lookbacks given the transparency and immutability of the ledger; and facilitate practical, technology-enabled KYC/CDD efforts, ongoing transaction monitoring, transaction tracking, and auditability/reporting.

Taking Action. Our Members are committed to compliance with Anti-Money Laundering ("AML"), countering the financing of terrorism ("CFT"), and sanctions laws and regulations, as applicable. We have been active participants in the Financial Action Task Force ("FATF") process to adopt Recommendations applicable to virtual assets and virtual asset service providers ("VASPs"). Our members have also dedicated significant resources to developing, implementing, and effectively maintaining AML compliance programs committed to promoting law enforcement objectives. Two examples of this real work commitment by the Chamber and its members are the Blockchain Alliance and the interVASP Messaging Standard.

> **The Blockchain Alliance**. The Blockchain Alliance, co-founded by the Chamber in 2015, is a proactive effort by the digital asset and blockchain industry to educate and support law enforcement and regulatory agencies.[3] With more than 115 participating companies and government agencies in the United States and around the world, the Alliance serves as an important medium for sharing information and education between the public and private sector to support law enforcement objectives. Policy makers should take note of the proactive work being done by the industry to ensure that law enforcement is knowledgeable about the industry and the technology to achieve its objectives, thus creating an orderly functioning of the marketplace. This work is being utilized by governments worldwide and can be further expanded to reach and assist more participants.
>
> **The interVASP Messaging Standard**. The Chamber is also a co-lead of the interVASP Working Group, a coordinated effort among the Chamber, Global Digital Finance, and IDAXA, three trade bodies with membership spanning industries and geographies (the "Joint Working Group") that developed a data messaging standard for use with the Travel Rule (the "IVMS101" or the "Standard"). Specifically, this Standard is a "[u]niversal common language for communication of required originator and beneficiary information between virtual asset service providers."[4] It is solely a data model that sets the rules and constraints for the information to be transmitted between originator and beneficiary (and intermediary, if applicable) VASPs.
>
> While a number of significant considerations must be developed to create a holistic solution for achieving compliance with the FATF's wire transfer

[3] BLOCKCHAIN ALLIANCE, https://blockchainalliance.org/ (last visited Nov. 24, 2020).
[4] Joint Working Group on interVASP Messaging Standards, *interVASP Messaging Standards*, interVASP.org (May 7, 2020), https://intervasp.org/wp-content/uploads/2020/05/IVMS101-interVASP-data-model-standard-issue-1-FINAL.pdf.

requirements applicable to VASPs, this Standard is focused solely around one aspect of that solution – the rules driving the actual data. It does not cover how that data is transmitted, security or privacy considerations, or other software-related implementations. Further, this Standard is designed to fit neatly into any of the software solutions developed or under development today as a complement to those efforts. As such, it is technology/protocol neutral. We understand that most, if not all, solutions currently on the market or in development have agreed to adopt the Standard.

The Need for a Competitive U.S. Industry. The increased costs described below – caused by a threshold far below what is recommended by the FATF – will also have the unintended consequence of putting the United States at a competitive disadvantage by helping to drive VASPs out of the United States into more favorable jurisdictions. From a national security perspective, China and others are years ahead of the United States in FinTech development; lowering the threshold risks driving business out of the United States while providing China, the EU, and many others a competitive advantage.[5]

III. Proposed Amendments to Definition of "Payment Order," "Transmittal Order," and "Money;" the Addition of New Definition "Convertible Virtual Currency"

a. The Need to Amend the Travel Rule

In our letter to FinCEN of November 26, 2019,[6] we set out the legal basis for why the Travel Rule does not apply to the virtual asset industry. We urged FinCEN to initiate a formal rulemaking process under the Administrative Procedure Act and, in so doing, obtain the benefit of industry feedback to consider how the Travel Rule can be enhanced to better fit this industry while achieving law enforcement objectives to obtain relevant information to stop illicit activity. As a result, we generally are supportive of this effort to amend the Travel Rule.

As we noted in our November 2019 Letter, "The text of the [Travel Rule] does not extend to transactions involving convertible virtual currencies ("CVCs"). Both FinCEN's prior analysis on this point and a comparison to a relevant section of the Uniform

[5] The Chamber has advocated for developing a National Action Plan for Blockchain to ensure that the United States remains a leader in technology. CHAMBER OF DIG. COMMERCE, NATIONAL ACTION PLAN FOR BLOCKCHAIN (Feb. 2019), https://digitalchamber.org/wp-content/uploads/2019/02/National-Action-Plan-for-Blockchain_.pdf. China's efforts to gain a competitive edge have been well-documented. *See, e.g.,* CHAMBER OF DIG. COMMERCE, DIGITAL YUAN PATENT STRATEGY: A COLLECTION OF PATENT APPLICATIONS FILED BY THE PEOPLE'S BANK OF CHINA (Feb. 2020), https://digitalchamber.s3.amazonaws.com/PBoC-Patents-Translated-Data.pdf.

[6] CHAMBER OF DIG. COMMERCE, *Comments to FinCEN Guidance: "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,"* FIN-2019-G001 (May 9, 2019) (Nov. 26, 2019), https://digitalchamber.org/wp-content/uploads/2019/12/Chamber-of-Digital-Commerce-Comment-Letter-to-FinCEN-Guidance1.pdf.

Commercial Code (the "UCC") demonstrate that the Rules apply only to transactions involving fiat currencies."[7] We concluded,

> "Money" is "a medium of exchange currently authorized or adopted by a domestic or foreign government" and therefore is limited to fiat currency. Because FinCEN does not consider virtual currency to have legal tender status, fiat currency or money cannot be virtual currency. Because virtual currency is not "money" as defined under UCC 4A, and the terms "funds transfer" and "payment order" in UCC 4A directly correspond to the terms "transmittal of funds" and "transmittal order" under the Rules (which expressly apply to "money"), the Rules as currently drafted cannot apply to transactions involving CVC.[8]

b. Proposed Definitions

As noted in the NPRM, the Travel Rule refers to a ''payment order'' (in the case of banks) and a ''transmittal order'' (in the case of financial institutions other than banks), concepts that both use the term ''money.'' As a threshold matter, the concept of "payment order" and "transmittal order" do not directly translate to the digital asset industry. When sending or holding value via blockchain technologies, no order for transmittal or payment needs to be placed between financial institutions because the information is available on the blockchain. Before applying the Travel Rule to an evolving technology with different functional mechanisms, the agencies should consider whether this rule is contextually accurate for new technologies, available now and anticipated in the future. Simply changing a definition does not make the Travel Rule functionally realistic for new technologies.

The NPRM seeks to expand the meaning of money beyond the UCC definition and define it in 31 CFR 1010.100(ll) (payment order) and 1010.100(eee) (transmittal order) to include: "(1) a medium of exchange currently authorized or adopted by a domestic or foreign government, including any digital asset that has legal tender status in any jurisdiction, or (2) a CVC."[9] The proposed rule would further define CVC as "a medium of exchange (such as cryptocurrency) that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status."[10]

As an initial matter, we question the proposal to define "money," a concept that is so fundamental to the financial system and is often defined similar to "currency," to include convertible virtual currency. Rather than taking an old rule that applied to transactions 25 years ago before digital payments existed, we suggest that the agencies instead take this opportunity to thoughtfully tailor the requirements to accomplish the core aims

[7] *Id*.
[8] *Id*. (citations omitted).
[9] NPRM, *supra* note 1, at 68,018.
[10] *Id*.

of the Travel Rule by considering drafting technologically-relevant obligations that actually match how digital assets are stored and how they move between entities in a blockchain environment.

Folding CVCs into the definition of money wholesale is imprecise and could lead to confusion in the application of the Travel Rule. To illustrate, in footnote 46 of the NPRM, the proposed rule states:

> The regulatory definitions of "money" and "convertible virtual currency" that this rulemaking proposes to add to the definitions of "payment order" and "transmittal order" at 31 CFR 1010.100(ll) and (eee) are specific to those provisions and not intended to have any impact on, inter alia, the definition of "currency" in 31 CFR 1010.100(m).
>
> Furthermore, nothing in this document shall constitute a determination that any asset that is within the regulatory definitions of "money" or "convertible virtual currency" that this rulemaking proposes to add to the definitions of "payment order" and "transmittal order" is currency for the purposes of the federal securities laws, 15 U.S.C. 78c(47), or the federal derivatives laws, 7 U.S.C. 1-26, and the regulations promulgated thereunder.[11]

By adding this footnote, the agencies acknowledge that changing the traditional definition of the term "money" could be confusing, both within the BSA and within the regulations of other agencies. Traditionally, the definition of both "money" and "currency" have been limited to the coin and paper recognized by a government as currency. Most state money transmitter statutes use two terms when a regulator wishes to regulate value in addition to money with the common phrase "money *or other monetary value*." By merging CVC into the definition of money for the limited purpose of applying the Travel Rule, the agencies will be introducing ambiguity rather than resolving it and risk confusing other instances where the term "money" is used elsewhere by making it unclear whether CVCs are in-scope—even where it is unintended. It also blurs the lines of what other types of value will now be considered money. Revising the definition of money, as proposed, could open the door to treating rewards points, frequent flyer miles, prepaid access, and other value the same as traditional currency.

This definition is also incongruent with FinCEN's previous positions. In FinCEN's 2013 Guidance, FinCEN made clear that CVC was not "legal tender."[12] Additionally, the

[11] *Id*. at 68,011 n.46.
[12] FIN. CRIMES ENF'T NETWORK, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FIN-2013-G001 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

Prepaid Access rule specifically states that the term "funds" does not include CVCs.[13] We agree that the definitions and the Travel Rule itself may need some adjustment, but recommend selecting some other approach, for example, by altering other definitions to include CVC instead.

If, however, FinCEN proceeds in amending the definition of "money," then, as a technical matter, we recommend that the definitions be refined to exclude a new term, "cryptocurrency," that is not defined, as follows:

> (2) For purposes of this paragraph (eee), the term ''money'' means: (i) A medium of exchange currently authorized or adopted by a domestic or foreign government, including any digital asset that has legal tender status in any jurisdiction. The term includes a monetary unit of account established by an intragovernmental organization or by agreement between two or more countries; or (ii) A convertible virtual currency.
>
> (3) For purposes of this paragraph (eee), convertible virtual currency means a medium of exchange ~~(such as cryptocurrency)~~ that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status.

We also note that there is no reference to CVC being a "digital" medium of exchange.

c. Further Clarifications to the Application of the Travel Rule to the Convertible Virtual Currency Industry

The challenges associated with developing a fully-functioning, cross-border information transfer system in a landscape where not all regulatory bodies globally have implemented regulatory frameworks, or may not value privacy and cyber security, in the same way as the United States is significant. Unfortunately, the Travel Rule and the FATF Recommendations expect U.S. exchanges to send customers' PII and commercially sensitive information to exchanges located in foreign jurisdictions who may not be registered or otherwise follow AML standards governing virtual assets or have no privacy or cybersecurity requirements in place to safeguard such sensitive information. This challenge is unique to virtual currency transactions, as there is no governing body that oversees the participants in the network in the same way that, for example, the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") oversees all institutions transacting on its network.

As a result, we urge FinCEN to consider the following when developing regulations and guidance related to the Travel Rule:

> 1. **Principles-based Approach**. Any enhancements to the Travel Rule should follow a principles-based approach that identifies FinCEN's underlying goals and

[13] Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45,403 (July 29, 2011), https://www.govinfo.gov/content/pkg/FR-2011-07-29/pdf/2011-19116.pdf.

works from there to identify potential solutions that achieve those goals. As demonstrated above, the new technologies available to VASPs can be helpful in enabling consistent and robust recordkeeping and KYC processes compared with traditional financial institutions, but the underlying technologies look and operate very differently than traditional financial institutions' order placement processes.

2. **Cyber Security and Privacy Considerations**. We suggest that FinCEN provide clarity on an appropriate way to deal with developing privacy obligations, such as the European Union General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") and hashing information on a blockchain for recordkeeping purposes (rather than storing it directly on a blockchain or DLT). In the course of providing clarity on specific compliance obligations under the CCPA, the GDPR and similar laws, FinCEN may also wish to consider how its application of the Travel Rule can best interact with the rights-based approach to privacy contained in such laws.

3. **VASP Discovery**. The owners of all wallets in existence are currently not universally known, nor is this likely to ever occur due to the frequency with which wallets can be created and the fact that they need not be created by a VASP. While data analytics software solutions provide an excellent picture of these accounts, it can still be difficult to ascertain whether a given wallet is hosted by a VASP or not. Similarly, while peer-to-peer data communications channels can allow the counterparties to a specific transaction to privately exchange information about a wallet address or transaction, such as if an address belongs to a VASP, these communications channels have not yet been universally deployed.

Moreover, when considering the custodian or financial institution supporting the wallet, often the customer may not know all of the financial institutions in the transaction, as many entities sub-custody their wallet services.

As a result, we request that FinCEN:

a. Provide guidance on how regulated entities can use alternative methods to verify information to help FinCEN achieve its goals by using the proper technological advances.

b. Provide guidance around when use of a more definitive response through a compliance data communications channel is recommended or required.

c. Confirm that entities are not responsible for collecting missing data from previous transactions (*i.e.*, the requirements are not retroactive).

d. Confirm that entities are not required to transmit information prior to or at the same time as the transaction, provided entities transmit information within a reasonable time frame after the transaction.

e. Confirm that if entities, after conducting reasonable steps, have no information to suggest that the counterparty is a VASP, they are able to assume that the transaction is not subject to the Travel Rule.

f. The price of CVC fluctuates against the U.S. Dollar, and transactions on a blockchain can take a number of minutes or even hours to be cleared or confirmed. We therefore request clarification of the responsibility of the financial institution if the transaction value subsequently increases above the threshold or decreases from the threshold amount.

    a. For example, *when* the USD-equivalent amount should be calculated and at what point of the blockchain clearing process:

        i. Whether this USD-equivalent amount is to be calculated at the point the transaction is broadcast by the originating VASP, or at the time the transaction is confirmed on the blockchain.

        ii. If the former, then additional guidance is needed with regard to the responsibility of VASPs in the scenario that the USD-equivalent value changes above/below the threshold between being broadcast and confirmed.

        iii. If the latter, then additional guidance is needed with regard to the number of confirmations required before the USD equivalent value is calculated.

    b. In addition, guidance is needed on the responsibility of VASPs in the scenario that a transaction is broadcast but remains in the mempool (the "waiting room" for transactions before they are successfully added into a block and added to the blockchain) for a sufficient period that, when added successfully into a block, the USD-equivalent value shifts above/below the threshold.

4. **Varying National Requirements**. Although FinCEN's proposed implementation of the FATF Recommendations only apply between VASPs, regulatory agencies such as the Swiss Financial Market Supervisory Authority ("FINMA") require information sharing for any transaction in which a VASP is involved. This is one example of the potential for divergent national implementation where the VASP requirements may vary. Thus, information flows

may also need to vary to meet those obligations. We recommend that FinCEN carefully consider the obligations imposed on VASPs by other nations in the context of its evaluation of changes to the Travel Rule.

5**. Engage Industry**. FinCEN has been excellent in maintaining a dialogue with industry, and we greatly appreciate its efforts to continue that dialogue through this and other public consultations. We recommend that FinCEN continue to engage industry through public private roundtables and town halls around the country, contemporaneous with the above, to better understand the efforts underway to build a holistic compliance network as well as how to better adapt the Travel Rule to achieve law enforcement objectives.

d. The Need for a Safe Harbor

We note that the Rules contain two components: (1) obtain and retain certain information, and (2) transfer that information. From a U.S. law enforcement perspective, FinCEN (and the Department of Justice ("DOJ"), where necessary) have the authority to seek information obtained and retained by U.S. money services businesses ("MSBs") (including VASPs) through the 314(a) process and, if necessary, by subpoena. The simple act of obtaining and retaining such information in a format available for law enforcement already serves as a benefit.

The challenge to complying with U.S.-specific transfer rules for companies utilizing blockchain/DLT is obtaining information held by non-U.S. MSBs offshore, prompting a burdensome process under mutual legal assistance treaties ("MLATs"). This is where the Travel Rule is convenient in that it requires non-U.S. VASPs to send information to U.S. VASPs when impacting a U.S. VASP's customer – thus subjecting that information to U.S. jurisdiction. What is not helpful to FinCEN is the vector by which U.S. VASPs send information to non-U.S. VASPs – outside the United States. (Although we recognize this action is very helpful to the receiving country.) Nevertheless, these tiered requirements, coupled with the uneven ramping up by member nations to apply the wire transfer provisions to VASPs, create an untenable and potentially dangerous circumstance for VASP customers whose data is being transmitted offshore to not yet FATF-compliant jurisdictions.

As a result, we suggest that FinCEN provide U.S. financial institutions with an exemption for transmitting data only until an operational system is in place. This "safe harbor" would be similar to exemptions provided by FinCEN when originally implementing the Travel Rule. For example, when elaborating on a safe harbor in 1998, FinCEN stated:

> FinCEN has made clear in the past that the purposes of the Travel Rule are not incompatible with flexibility in applying the Rule's literal terms. The need for administrative flexibility is increased because Treasury intends, within the next 18 months, to review and consider making appropriate

> modifications to the Travel Rule. See 61 Fed. Reg. 14,383, 14,387-88. Modifications are appropriate to meet particular operating problems, so long as complete information is available, at some point, in the domestic funds transfer chain and investigators are given adequate notice that the funds transmittal order itself must be supplemented by other information to provide a complete picture of the transmittal involved.[14]

Much progress has been achieved in the past year, and full implementation should be achieved efficiently such that the exemption would no longer be needed in the near future. As the system comes online globally, FinCEN, and perhaps Congress, should consider a limitation of liability for U.S. financial institutions to provide a clear exemption from lawsuits (whether private or brought by government, *e.g.,* under CCPA or the GDPR) for sharing information required under the BSA. This can be similar to the limitation of liability offered for suspicious activity reporting at, for example, 31 C.F.R. 1022.320(e).

IV. Proposed Reduction of Recordkeeping Threshold

The NPRM proposes to lower the dollar threshold of the existing requirements in 31 CFR 1020.410(a) and 31 CFR 1010.410(e) and (f) to collect, retain, and transmit information on funds transfers and transmittals of funds in amounts of $3,000 or more to $250 for funds transfers and transmittals of funds that begin or end outside the United States.

The proposed ***92%*** reduction in the threshold for this recordkeeping requirement for cross-border transactions would significantly increase the burdens on financial institutions. In addition, there is little benefit to be gained from an information/data gathering standpoint for regulated exchanges since exchanges and regulators and law enforcement already have a high level of clarity to see all on-chain transactions without the Travel Rule, and regulated exchanges are already obligated to gather robust customer information. Finally, financial intelligence units ("FIUs") such as FinCEN should be seeking to include as many participants within the regulated financial system

[14] Conditional Exceptions to Bank Secrecy Act Regulations Relating to Orders for Transmittals of Funds by Financial Institutions, 63 Fed. Reg. 3,640-41 (Jan. 26, 1998); *see also*, Amendment to the Bank Secrecy Act Regulations Relating to Orders for Transmittals of Funds by Financial Institutions, 61 Fed. Reg. 14,386 (Apr. 1, 1996)(amending the Travel Rule to acknowledge that "until all banks convert to the expanded Fedwire format, there will not always be enough space to include in a transmittal order all of the information required by the Rule." As a result, FinCEN incorporated an interim exception to the Travel Rule such that, "until it has converted to the new Fedwire format, a financial institution will be deemed to be in compliance with paragraph (g), even if some information required to be included on a transmittal order is not so included…." The forbearance was permitted with conditions: "provided that, when either requested by a corresponding financial institution to assist in retrieval of information in connection with Bank Secrecy Act compliance efforts or in response to a law enforcement request, or when presented itself with a judicial order, subpoena or administrative summons requesting any information required by paragraphs (g)(1)(i), (g)(1)(ii), (g)(1)(vii), (g)(2)(i), (g)(2)(ii), or (g)(2)(vii), the financial institution retrieves such information within a reasonable time." *Id*. at 14,387.

– lowering the threshold will negatively impact financial inclusion within these frameworks, reducing visibility not increasing it, as discussed below.

a. Insufficient Time to Calibrate Resulting Costs

As a starting point, the 30-day comment window provided in the NPRM is insufficient time for affected entities to calculate with precision the magnitude of the impact of this lower threshold. We urge FinCEN and the Board to carefully consider important changes such as this without meaningful industry feedback, and we request an extension of time in which to respond to the varied consequences of this change. This reduction will require significant technical and personnel adjustments – not only in customer onboarding functions, but also corresponding sanctions screening, monitoring and reporting functions, processes that are already proven to be onerous, creating numerous false positives requiring investigation and documentation to conclude.

b. A 92% Threshold Reduction Creates Significant Increased Burdens with Little Corresponding Benefit

A 92% decrease in the recordkeeping threshold creates an exponential increase in compliance costs that reverberate throughout compliance systems beyond the initial widening in scope of the number of transactions.

1. Volume of Transactions Affected[15]

Our Member CipherTrace, a blockchain analytics firm, has calculated that the volume of required U.S. VASP Travel Rule messages will increase 250% in volume alone. The following chart shows transactions in bitcoin for the month of October 2020.

[15] With more time to comment, we could run different variables to the searches to identify more specific data sets.

Number of Travel Rule Messages Required by U.S. VASPs

Monthly Transactions

Region	Txs Over 250	Txs Over 1000	Txs Over 3000	Current 3000	Proposed Change
US Domestic	15,921	11,016	7,510	7,510	7,510
Cross US Border	79,011	46,780	27,295	27,295	79,011
International	392,952	260,439	178,664		
Global	487,884	318,235	213,469		
Monthly Travel Rule Correspondences	-	-	-	34,805	86,521
Annual Travel Rule Correspondences	-	-	-	417,660	1,038,252

2. Associated Costs

Affected institutions will incur the following categories of costs, among others, which are difficult to calculate, particularly in the 30-day window provided. This includes, but is not limited to:

- Cost of API calls to a bulletin board or other Travel Rule solution, which will increase by the number of net new transactions subject to the Travel Rule.
- Sanctions screening that must be performed on the data received, which is typically charged on a per-name basis. In addition, sanctions screening typically results in a high number of false positives that must be manually reviewed. In addition to the personnel costs associated with reviewing screening alerts, institutions will need to freeze customer accounts while the alerts can be reviewed. This will cause significant customer friction, especially since cryptocurrency transactions operate 24/7.

There can be no doubt that these increased costs will be significant and, in many cases, are unique to the convertible virtual currency industry.

It should be noted that it is difficult to determine accurately the location of a particular transaction, especially where a VASP may have more than one legal entity globally. This means, as a practical matter, that VASPs will need to consider all transactions at $250 to be subject to the Travel Rule. Similarly, since the name and address of the recipient do not need to be collected to effect a virtual currency transaction, it is unlikely

that VASPs will receive this information with the so-called "transmittal order," and will therefore not be able to retain the record.

3. Effective Compliance

Considerations around BSA recordkeeping requirements have typically centered on how to better streamline compliance "to allocate resources more effectively."[16] For example, FinCEN believes that the proposed regulatory approach in its recent advanced notice of proposed rulemaking ("ANPRM") seeking to enhance AML program effectiveness furthers the statutory BSA purpose of providing information with a high degree of usefulness to government authorities.[17]

FinCEN's ANPRM further states that,

> The AMLE WG recommended that AML monitoring and reporting practices be modernized and streamlined to maximize efficiency, quality, and speed of providing data to government authorities with due consideration for privacy and data security. The AMLE WG recommended that the relevant government agencies consider:
>
> - Clarifying expectations and updating practices for keep-open letters and suspicious activity monitoring, investigation, and reporting, including SARs based on grand jury subpoenas or negative media; and
>
> - Supporting potential automation opportunities for high-frequency/low-complexity SARs and currency transaction reports (CTRs), and exploring the possibility of streamlined SARs on continuing activity.[18]

Reduction of the threshold to below $3000 contradicts the intent of maximizing efficiency and speed of data with appropriate consideration for privacy and data security.

In addition, the Department of Justice ("DOJ") has specifically noted in its June 2020 update to Evaluation of Corporate Compliance Programs that companies are expected to execute "risk-tailored resource allocation" and avoid "devot[ing] a disproportionate amount of time to policing low-risk areas instead of high-risk

---

[16] Press Release, Fin. Crimes Enf't Network, FinCEN Seeks Comments on Enhancing the Effectiveness of Anti-Money Laundering Programs (Sept. 16, 2020), https://www.fincen.gov/news/news-releases/fincen-seeks-comments-enhancing-effectiveness-anti-money-laundering-programs.
[17] FIN. CRIMES ENF'T NETWORK, Anti-Money Laundering Program Effectiveness, 85 Fed. Reg. 58,023, 58,027 (Sept. 17, 2020), https://www.govinfo.gov/content/pkg/FR-2020-09-17/pdf/2020-20527.pdf (hereinafter, the "ANPRM").
[18] *Id*. at 58,025.

areas...."[19] By lowering the thresholds, VASPs will inherently be forced to dedicate a portion of their finite resources to monitoring a great population of transactions that typically present lower risk.

This NPRM moves in the opposite direction of the goals of that contemporaneous ANPRM and DOJ expectations and creates more recordkeeping requirements.

c. Credit Card Transactions Settling in Convertible Virtual Currency are Unfairly Impacted by the Threshold Change

Card networks and other card processors are typically excluded from the definition of money transmission and, therefore, the Travel Rule. This is, in part, because both the card issuer and the acquirer are regulated institutions that operate an account-based model and, therefore, the identity of the transmittor and recipient are subject to KYC by default. It would be extremely burdensome for the processor, that has no relationship with the cardholder, to identify the purchaser in a point of sale transaction.

However, FinCEN previously ruled that where credit card transactions settle in virtual currency, the transaction is, in fact, money transmission. [20] A number of VASPs process credit card transactions on behalf of their customers, who are merchants. These credit card transactions are settled in virtual currency into accounts held by the merchant at the VASP, which is a duly regulated financial institution.

The proposed change to the Travel Rule threshold would result in these VASPs having to identify the cardholder for a point of sale transaction. For example, if an individual wished to purchase a pair of shoes for $255.00 at a merchant that has elected to settle their transactions in convertible virtual currency, the individual would have to provide their identity, including social security number, to the merchant in order to purchase the shoes, despite the fact that the individual is blind to the fact that the merchant has elected to settle their transactions in virtual currency.

The fact that these transactions are considered money transmission subject to the recordkeeping and Travel Rules, when the same transaction settling in fiat is not, already places VASPs at a disadvantage compared to other credit card processors. The reduction in threshold disproportionately impacts VASPs conducting these transactions. One Chamber Member VASP's analysis of their credit card processing transactions suggests that a reduction in the threshold to $250 will result in an increase in the number of transactions subject to the Travel Rule of 82,500%, with the number of unique transmittors increasing by 73,000%.

---

[19] U.S. DEP'T OF JUSTICE, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, 3 (JUNE 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download.

[20] FIN. CRIMES ENF'T NETWORK, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf.

d. Changes to the BSA Should Emphasize Fostering Financial Inclusion of the Unbanked and Underbanked

One consequence of these dramatically increased burdens will be to increase the cost of convertible virtual currency-related transactions, including remittances, which undermines the goal of financial inclusion. Lowering the threshold will have the negative effect of promoting financial *exclusion*, driving out those persons from the regulated financial system who will have cheaper and easier alternatives to the new structure.

- An important objective to prevent money laundering should be to provide for the increased engagement of financially underserved, de-risked and/or excluded parties into the formal financial services sector to reinforce the fact that a *more inclusive* financial system is more *effective* in protecting against financial crime. Notably, financial exclusion and de-risking practices have disproportionately impacted certain segments of the economy with profound consequences on the ability to ensure one's own financial stability and economic security. De-risking due to increasing AML/CFT requirements have been particularly harmful to cross-border remittances, a noted lifeline of millions of people and numerous corridors whose livelihoods and economic wherewithal depend on these flows.

- This NPRM moves to reverse financial inclusion by placing additional burden in record keeping on institutions serving low-income individuals who tend to transfer funds at or under the newly proposed threshold. We argue that the losses resulting from the lack of inclusion and, by extent, the associated transparency, outweigh potential law enforcement benefits, thus not solving the national security challenge.

- Current AML/CFT practices should be evaluated for their *effectiveness* in accomplishing the twin aims of financial inclusion and the protection of system integrity. An *effective* AML/CFT regime should extend its scope to apply to those financially underserved or excluded from the traditional financial sector. In short, effective programs should reflect the engagement of more legitimate actors in addition to preventing illicit activities and the exploitation by illicit actors.

- Indeed, global standards and evaluations have already moved in this direction. In 2013, the FATF acknowledged that "reasonable legal frameworks" to prevent financial crime were no longer sufficient. [21] The FATF stated that "each country must enforce these measures, and ensure that the operational, law enforcement and legal components of an AML/CFT system work together

[21] FATF, Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (Oct. 2019), http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

effectively to deliver results: the 11 immediate outcomes."[22] This resulted in the FATF amending its mutual evaluation process of member states. Further, the FATF explicitly stated that financial inclusion "also expands the scope of traceable transactions, facilitating the detection, reporting and investigation of suspicious transactions, thereby reducing overall money laundering (ML) and terrorist financing (TF) risks. Financial inclusion and financial integrity are thus mutually reinforcing."[23] Financial inclusion outcomes should be explicitly evaluated alongside those technical aspects related to the legal framework, system operations, and enforcement mechanisms of an AML/CFT regime in assessing effectiveness.

The Chamber is concerned that this change will have unintended discriminatory consequences for lower income populations and immigrants. Lower income populations rely on the ability to conduct lower value transactions that would be included within a threshold of $250. In particular, we urge the agencies to consider the direct and disproportionate impact the proposed rule would have on millions of immigrant communities with family abroad that send money back to families and loved ones in low and middle-income countries.[24] These remittances help families from some of the world's poorest communities afford food, healthcare, and basic needs, and have become increasingly important as a source of external financing.[25] These immigrant communities already contend with some of the most significant transaction costs, with the average cost of remittances being 6.8%, with the average cost for Sub-Saharan Africa being about 9%. Data on remittances is not uniform, but it is indisputable that the lower proposed threshold will bring millions of ordinary remittance transactions within the scope of the Travel Rule, and, given the absence of any inflation-linked threshold, millions more will be brought into scope over time.[26] In fact, it is possible, if not

---

[22] FATF, *Mutual Evaluations, An Effective System to Combat Money Laundering and Terrorist Financing*, https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html (last visited Nov. 24, 2020).

[23] FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, FATF (Nov. 2017), http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf.

[24] Data and information on the scale of remittance transfers, as well as up-to-date statistics and trends, can be found from the United Nations and Organisation for Economic Co-operation and Development. *See*, *e.g.*, MIGRATION DATA PORTAL, Remittances, https://migrationdataportal.org/themes/remittances#key-trends (last updated Nov. 17, 2020); *see also*, ORGANISATION FOR CO-OPERATION AND DEVELOPMENT, REMITTANCES AND DEVELOPMENT, https://www.oecd.org/dev/americas/42716118.pdf (Pablo Fajnzylber and J. Humberto López eds., 2008).

[25] *See* Press Release, The World Bank, Record High Remittances Sent Globally in 2018 (Apr. 8, 2019), https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018; *see also*, The World Bank, World Bank Predicts Sharpest Decline of Remittances in Recent History (Apr. 22, 2020), https://www.worldbank.org/en/news/press-release/2020/04/22/world-bank-predicts-sharpest-decline-of-remittances-in-recent-history. Understandably, the recent decline of remittances in 2020 was predominantly caused by the macro-economic factors of the COVID-19 pandemic and should not be viewed as a determinant of the broader trend, over decades, of increasing remittance flows.

[26] *See, e.g.,* Government Accountability Office, International Remittances: Different Estimation Methodologies Produce Different Results (Mar. 2006), https://www.gao.gov/new.items/d06210.pdf. The majority of statistical analysis performed by the World Bank and International Monetary Fund regarding remittance transactions use $200 as an average amount for calculating remittance costs. We note that

probable, that the majority of transactions that "begin or end in the United States" within the threshold will be remittance transactions.

By contrast, maintaining a threshold of $3,000 for cross-border transfers would be consistent with prior practice and the build out of compliance programs across all types of financial institutions for almost 25 years. This consistency is most critical at a time when the industry is building out a solution for a global information transfer system. **Implementing a new compliance standard that *requires* financial institutions to share sensitive customer information with unaffiliated third parties presents significant challenges. It cannot be understated the important concerns that must be addressed in such a system – both the privacy and cyber security protections of user data (both individuals and corporate) must be protected.** To the extent there are law enforcement interests in tracking information associated with suspicious lower-dollar transactions that cross borders, those objectives can be achieved using current KYC/CDD practices, SAR filings, and other existing recordkeeping and reporting obligations, without creating undue burdens on VASPs and their customers and unwanted impacts on U.S. commerce.

* * *

Thank you for the opportunity to comment on the proposed amendments. We look forward to collaborating FinCEN and the Board in further endeavors to enhance their law enforcement objectives in a meaningful and effective way. Further, we are happy to answer any questions related to these comments and to serve as a resource on these topics.

Very truly yours,

Amy Davine Kim
Chief Policy Officer

---

this is an average amount, indicating that some transactions are for amounts higher than this (and thus would be captured by the proposed threshold revision of $250) and some are for lower amounts. Even in 2006, some immigrant communities, such as adult foreign-born Hispanics, remitted monthly amounts that would have exceeded the proposed threshold. *See id.* at 19 (finding "70 percent of percent of adult foreign-born Hispanics remit and on average, they remit $3,024 per year").