CHAMBER OF DIGITAL COMMERCE

March 31, 2020

Via Email

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

Re: Update on InterVASP Messaging Standard; Follow up Perspectives on Funds Travel and Transfer Rules; and Next Horizon Issues

Dear Director Blanco,

The Chamber of Digital Commerce (the "**Chamber**") welcomes the opportunity to follow on our letter dated November 26, 2019, and our subsequent conversations for consideration by the Financial Crimes Enforcement Network ("**FinCEN**"). This letter contains the following: 1) an update on the Chamber's work within the InterVASP Messaging Standard; 2) follow up considerations and proposed action items for implementing the Funds Travel and Transfer Rules (the "**Rules**"); and 3) further discussion of "next horizon" issues.

I. InterVASP Messaging Standard – IVMS101

The Chamber is a co-lead of the InterVASP Messaging Standard ("**IVMS101**"), a coordinated effort among the Chamber, Global Digital Finance, and IDAXA, three trade bodies with membership spanning industry and geographies (the "**Joint Working Group**"), to develop a data messaging standard (the "**Standard**"). Specifically, this Standard will be a "*Universal common language for communication of required originator and beneficiary information between virtual asset service providers.*" 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 wire transfer requirements, 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.

The Joint Working Group overseeing the work is significant because it brings together industry representatives from across disciplines and geographies, demonstrating that this industry is working together to achieve solutions. We were deliberate in the types of participants we recruited. While open to everyone, our focus was to draw participants from VASPs, primarily, as well as other obliged entities undertaking virtual asset activities, academics, technical solution providers, standards-setting bodies, and supervisors/regulators of VASPS. In this regard, we have invited members of your team to participate as observers to stay informed of our work.

Today, the Joint Working Group is comprised of over 115 technical experts, of which 59 are members – that is, those that may be directly impacted by, and regulated under, the newly updated Recommendations. The goal is to bring together a diverse group to develop a universal standard that is capable of being adopted by industry as a single solution to the format and rules of the data.

The group started its work in December and has conducted 12 of its 18 expected meetings, to wrap up drafting by the end of April in time to present a draft to the FATF for consideration in their upcoming implementation report. We hope to finalize the Standard in May 2020. At that time, the industry groups will convene with their members to encourage adoption.

II. Next Steps Regarding the Funds Travel and Transfer Rules

In our letter to you of November 26, 2019, we set out the legal basis for why the Rules do not lawfully apply to the virtual asset industry at this time. 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 Rules can be enhanced to better fit this industry while achieving law enforcement objectives to obtain relevant information to stop illicit activity.

In this regard, we also reiterate the challenges associated with developing a fully-functioning system in a landscape where regulatory bodies have not yet implemented licensing or registration regimes, or may not value privacy and cyber security in the same way as the United States. Unfortunately, the FATF Recommendations expect U.S. VASPs to send personally identifiable customer information to VASPs located in

foreign jurisdictions, who may not have registered or otherwise follow AML standards around virtual assets.

As a result, we urge the following considerations when developing a notice and comment consultation:

1. **Principles-based Approach**. Any enhancements to the Rules should follow a principles-based approach that identifies FinCEN's underlying goals and works backwards to identify potential solutions.

2. **Cyber Security and Privacy Considerations**. We suggest that FinCEN provide clarity on an appropriate way to deal with developing privacy obligations, such as GDPR, and hashing information on a blockchain for recordkeeping purposes.

3. **VASP Discovery**. It is currently not universally known the owners of all wallets in existence. 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. As a result, we request that FinCEN:

    a. Provide guidance on how regulated entities can use blockchain analytics tools as a primary or secondary check to verify information.
    b. Clarify the responsibility of an entity if the information is sent but is unable to be received by the counterparty. A VASP should not be responsible for receipt of information by the receiving institution (absent significant factors).

    c. Whether entities are responsible for collecting missing data from previous transactions.

4. **Varying National Requirements**. Although FinCEN and FATF requirements only apply between VASPs, regulatory agencies such as FINMA require information sharing for any transaction in which a VASP is involved. This is one example of the potential for national implementation where the VASP requirements may vary. Thus, information flows may also need to vary to meet those obligations.

5. **Engage Industry**. We recommend that FinCEN 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 Rules to achieve law enforcement objectives.

We note that the Rules contain two components: obtain and retain certain information and transfer that information. From a singularly U.S. law enforcement perspective, FinCEN (and the Department of Justice, where necessary), have the authority to seek information obtained and retained by U.S. VASPs through the 314(a) process and, if

necessary, by subpoena. The challenge is obtaining information held by non-U.S. VASPs offshore, prompting a burdensome process under the MLATs. This is where the second component of the Rules 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 wire transfer provisions to VASPs, create an untenable and potentially dangerous circumstance for VASP customers whose data is being transmitted offshore.

As a result, we suggest that FinCEN provide U.S. VASPs 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 Rules. 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.[1]

[1] 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.

Given the progress noted above, and our willingness to keep FinCEN apprised of our progress, full implementation should be achieved efficiently such that the exemption should no longer be needed.

As the system comes online globally, FinCEN, and perhaps Congress, should consider a limitation of liability for VASPs to provide a clear exemption from lawsuits (whether private or brought by government, *i.e.,* under GDPR) for sharing information required under the Bank Secrecy Act ("**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).

III. Consideration of "Next Horizon" Issues

As mentioned in our November 26 letter, we have identified a number of issues that we foresee to gain importance as the VASP industry evolves – what we call "next horizon" issues.

a. Development of KYC utility for cost efficiency and effective customer onboarding. Current rules only allow reliance on third party KYC if it was conducted by a regulated affiliate. This would need to be reconsidered and expanded to allow for such a utility.

b. Whether the 314(a) and 314(b) process for information sharing between government agencies, industry, and financial institutions should be enhanced, and the implications for VASPs.

c. Clarity on how the BSA applies to Decentralized Applications that are neither operated by a financial institution nor any centralized party or group.

d. Use of blockchains for recordkeeping purposes and other ways to implement "RegTech" for BSA compliance.

e. Use of privacy coins to solve privacy issues while still achieving AML compliance. This would include whether firms can increase due diligence measures to address "anonymity" concerns and ways wallet providers can address incoming transactions in privacy coins.

f. Regulatory considerations over when mixers and tumblers have been used in a token's transaction history.

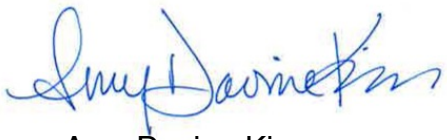
g. OFAC and AML considerations when transaction histories can be traced back many "hops," which is not true for fiat-based transactions. How far back must a financial institution go to meet AML compliance obligations, keeping in mind that current guidance does not require financial institutions to know their customer's customer? Can blockchain analytics software provide appropriate information to satisfy KYC and transaction monitoring obligations?

To address these topics, we propose that FinCEN publish a request for consultation to learn more from industry on their perspectives in these areas and others. We would be pleased to enhance these topics further if helpful in this regard.

* * *

We greatly appreciate your consideration of these issues, and look forward to continuing our dialogue to detect, deter, and prevent illicit activity.

Very truly yours,



Amy Davine Kim

cc: Michael Mosier
Felicia Swindells
Carole House