April 8, 2019
Secretariat
Financial Action Task Force
FATF.Publicconsultation@fatf-gafi.org

To Whom It May Concern:

We appreciate the opportunity to offer comments to the Financial Action Task Force (FATF) regarding the Interpretive Note to Recommendation 15, in particular paragraph 7(b) that states "countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, *submit the above information to beneficiary VASPs and counterparts (if any)*, and make it available on request to appropriate authorities."

We thank the FATF for this public consultation and hereby provide the input from Chainalysis based on our industry and technical expertise as well as contribution from clients and partners at roundtable discussions on this topic in San Francisco, New York, and Seoul, and global conference calls. We will focus our comments most notably on the italicized portion above.

**Introduction**

Virtual assets were invented to reduce the dependence on intermediaries in financial transactions. Indeed, the original whitepaper outlines Bitcoin as a peer to peer financial system that has no central authority and no intermediaries. This poses a unique challenge for financial regulators, as they have traditionally deputized monitoring to regulated intermediaries.

The good news is that virtual assets operate on public ledgers that offer greater transparency than traditional financial systems, and blockchain analytics and forensic tools have a track record of helping to foster industry cooperation in tackling illicit activity. Therefore, we believe these capabilities allow for a new regulatory approach that preserves the integrity of this new global financial system.

We are providing input to Recommendation 7(b) noting:

1. **Technical limitations:** Virtual Assets are designed to provide a way to move value without the need to identify the participants in a transaction. In fact, in most circumstances, VASPs are unable to tell if a beneficiary is using a VASP or their own

personal wallet in any given transaction. Therefore, requiring a transmission of information identifying the parties is not feasible.

2. **Technical opportunities:** VASPs can use the transparency of the shared ledger to form an effective risk based approach. VASPs should collect and store Know Your Customer (KYC) information on the identity of the originator. While the transactions themselves are public, VASPs must link their customers with their specific transactions as this information is not available on the public ledger. Independent observers, including regulators, law enforcement, and banks, can leverage blockchain analytics tools to identify suspicious activity and mitigate money laundering, terrorism financing, and other illicit activity. Chainalysis has helped track billions of dollars of stolen funds and illicit activity.

3. **Unintended Consequences:** There is no infrastructure to transmit information between VASPs today, and no one has the ability to change how virtual asset blockchains work. Forcing onerous investment and friction onto regulated VASPs, who are critical allies to law enforcement, could reduce their prevalence, drive activity to decentralized and peer-to-peer exchanges, and lead to further de-risking by financial institutions. Such measures would decrease the transparency that is currently available to law enforcement.

This letter is divided into the following sections:

I. Architecture of Virtual Assets

II. Tracing: The Art of the Possible

III. Implementing Controls, De-risking and Regulatory Arbitrage

IV. Clarifications and Recommendations

## I. Architecture of Virtual Assets

Virtual Assets are global in nature. Ownership of these assets is recorded on ledgers that are accessible anywhere at any time. Transfers of ownership from one individual to another are simply entries in these global ledgers.

Virtual Asset ledger entries are irreversible and almost instantaneous, regardless of geography. These transfers happen when an originator broadcasts a transfer to the entire network, and the entry is recorded. Anyone on the network can send virtual assets to anyone else. There is usually no way for the recipient to block payments, with the exception of certain virtual assets

such as some stablecoins that have implemented controls on the blockchain protocol that allow them to freeze assets.

VASPs make up a considerable portion of the entries into virtual asset ledgers. In fact, VASPs facilitate hundreds of thousands or even millions of transactions daily. This requires systems to automate the monitoring and processing of these transactions. Therefore, information sharing on these transmissions would also have to be automated. Despite the prominence of VASPs, there is also a considerable amount of peer to peer (P2P) transactions, and the regulation of VASPs should not be made in isolation of the technology's original purpose to facilitate P2P transactions.

Virtual assets create a global settlement layer that increases the availability of financial services to the world. With an open architecture, new businesses and financially disenfranchised people can access financial services. With lower switching costs between service providers, it also fosters competition to improve offerings to consumers.

## II. Tracing: The Art of the Possible

Unlike cross-border wire transfers, blockchains perfectly preserve the provenance of financial transactions and do not suffer from data integrity issues. Before Chainalysis was founded in 2014, investigators made their own systems to track blockchain transactions. With just the Bitcoin ledger and seized devices, they were able to prove financial benefit in cases such as the United States of America v Ross Ulbricht, the administrator of the darknet market Silk Road.

Now, commercial blockchain intelligence software companies such as Chainalysis map blockchain transactions to real world entities. This does not mean we handle personally identifiable information (PII) on end users, but we can use pseudonymous blockchain identifiers to estimate the source and destination of funds between entities and services such as VASPs, ransomware campaigns, and darknet markets. Law enforcement can use these pseudonymous identifiers to legally request identifying information from either the receiving or sending VASP. The pseudonymous nature of this information also affords a level of velocity in information sharing that was not previously possible due to data protection and data privacy laws.

Unlike traditional finance, which relies on typologies to identify potentially suspicious activity, bad actors often advertise their virtual asset addresses. For example, ransomware perpetrators openly supply their virtual asset addresses. Chainalysis collects these addresses for law enforcement, VASPs, and banks to coordinate their efforts to disrupt this activity.

Law enforcement, regulators, financial institutions, and cryptocurrency businesses all leverage Chainalysis's services to understand the underlying activity behind transactions:

- VASPs use our compliance software to identify the underlying risk of transactions. VASPs can screen transactions in real time to know whether they are about to send virtual assets to an address that has been linked to illicit activity.
- Law Enforcement can proactively build cases without suspicious activity reports based on illicit activity identified in our products.
- Regulators are able to inspect transactions without reports of suspicious activity from VASPs. They can also enhance the intelligence that is included within reports with additional intelligence collected from Chainalysis's proprietary or public sources.

As transactional records are public, VASPs and financial institutions are able to access indicators of suspicion beyond the information they collect from their customers. Our customers in over 40 countries around the world are able to collaborate on investigations and access the same transactions. We have participated in several international takedowns of large criminal enterprises, such as Hansa, once the largest darknet market in Europe. In many of these cases, one of the biggest barriers was the inefficiency of the Mutual Legal Assistance Treaty (MLAT) system.

Despite these significant technical differences between virtual assets and traditional cross-border money transfers, 7(b) as it is currently drafted would lead them to be regulated in essentially the same way. One customer of ours suggested that VASPs are more analogous to broker dealers as asset traders than wire transfer services, which we discuss later in section IV.

Given the architectural benefits of virtual assets, we call upon FATF to assist Financial Intelligence Units (FIUs) around the world in bringing information sharing standards in line with the speed of transactions. Such measures would enhance law enforcement's abilities to combat global threats.

**III. Implementing Controls, De-risking and Regulatory Arbitrage**

Virtual Assets have been regulated in some jurisdictions since FinCEN issued guidance in 2013. This paved the way for other countries to follow suit and recognize the role of virtual assets in money transmission.

Law enforcement has successfully dismantled many of the largest darknet markets, such as Alphabay and the previously mentioned Hansa and Silk Road. Coordination of these large cyber investigations were made possible by easy access to these marketplaces' financial transactions and facilitated by subpoenas to VASPs in the various countries where law enforcement arrested and prosecuted administrators, vendors, and users.

A consequence of improved anti-money laundering/combating the financing of terrorism (AML/CFT) regimes in the traditional financial services sector is “de-risking,” the restriction or termination of banking services to high risk institutions and services or to entites in high risk jurisdictions.

The impact of “de-risking” is substantial. Persons and organizations in said jurisdictions lose access to regulated financial services, and must turn to underground banking. This is the worst possible scenario for financial crime mitigation because transactions on unregulated channels eliminate transparency.

De-risking is on the rise, and would significantly alter the virtual assets ecosystem. Organizations that generate low volumes while presenting significantly higher AML/CFT risks are the most vulnerable. Many VASPs would fall within this category, resulting in the loss of banking relationships, and ultimately, the closing of their businesses, regulatory arbitrage, or underground banking. These VASPs, already struggling to gain access to banking services, would have no choice but to become more opaque and contribute to even greater AML/CFT challenges.

Given the global nature of the technology, the risk of regulatory arbitrage is particularly acute. Some jurisdictions may interpret some entities to be pure technology providers while other jurisdictions may consider the same entities to be VASPs. In such cases, the flight of VASPs to friendlier jurisdictions will decrease regulators’ visibility into the underlying activity. Greater clarity from FATF on what constitutes a VASP will mitigate the risk of regulatory arbitrage.

**IV. Clarifications and Recommendations**

*Clarifications*

Based on our conversations with VASP customers, we’ve identified a substantial gap in awareness and understanding of the 7(b) draft and how it would impact their businesses. Additionally, we, with input from our customers, identified areas where specific clarification from FATF would be beneficial.

1. Definition of VASP

   While some VASPs operate like money services businesses, some of our customers’ businesses resemble broker-dealers. In other words, some VASPs specialize in transmitting value person to person, while many more operate like asset traders. As such, there are increasing calls for VASPs to be regulated as broker dealers in the US.

   Not all VASPs have identifying information on the ultimate beneficiaries. This is not due to a lack of controls, but rather is the nature of their businesses. Much of virtual asset activity is speculative rather than involved in money transmission, and the confidentiality

of the party behind trades is essential for market stability. Any regulations should consider the variety of business models that are prevalent among VASPs.

This raises the following questions: How does FATF define VASP? Should the same rules apply to all VASPs, regardless of their business models?

Further, treating all VASPs as money services businesses presents challenges. For example, in the broker-dealer industry, systems and processes exist to protect the market from potentially destabilizing information flows. Dark pools and omnibus accounts prevent traders from tipping the market when they may be building market-making positions. The imposition of 7(b) on the virtual asset industry would require VASPs to transmit identifying information, making the market vulnerable to destabilizing information flows.

Finally, as 7(b) is currently written, it is unclear if there is protection for software developers who build virtual asset wallets that allow individuals to manage their own wallets and transmit virtual assets to and from them. We suggest FATF clarify that these engineers are not considered VASPs and therefore are immune from the requirements set forth in 7(b).

2. Implications with Respect to Privacy Laws

Increasingly stringent data privacy and data protection laws are coming into effect across multiple jurisdictions, including Europe's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the India Draft Data Protection bill. For example, GDPR dictates that organizations that control personally identifiable information (PII), such as financial services providers, are obligated to facilitate the privacy rights granted under the regulation.

These laws create barriers to data flow and make AML/CFT programs more difficult to execute. While it is generally understood that more leeway is granted in relation to data transmission to fight financial crime, this has not yet been formally defined in legislation. Specifically, it is unclear what warrants the legal basis for transmission.

As such, has the delegation considered how 7(b) will work with current and future privacy laws? Will the implementation of 7(b) require a closed network with standards like SWIFT in order to comply with these laws?

The scope of building such a platform would be incredibly costly and time intensive to initiate. Even if it were created, there would be issues such as how data is stored and the membership criteria to join such a platform. Further, it would be impossible to enforce; the creators of every virtual asset address would have to register each address they control. The end result would be an incomplete system with diluted efficacy.

*Recommendations*

Given the technical infeasibility of 7(b) as it is currently written, we recommend the following:

1. VASPs should be regulated and registered at the appropriate authority, obliged to identify their customers and maintain records on which cryptocurrency transfers were associated with each customer, and required to provide information when requested, similar to domestic payment systems.

2. Originator VASPs should screen destinations for known illicit activity using an automated monitoring system and manage a customer due diligence (CDD) program for transactions that trigger risk thresholds based on detected illicit activity.

3. Beneficiary VASPs should understand the source of funds when possible using an automated monitoring system.

4. Private individuals, whether originator or beneficiary, should not be expected to register or be licensed unless it is their business to transfer or sell virtual assets.

5. The USD/EUR 1000 threshold is low and should be raised. We heard from customers that this would be especially onerous for them. Further, given the volatility of the virtual asset markets, a VASP that would normally be outside the scope of these requirements could suddenly be subject to them, and may not have the infrastructure to support.

6. We fully support the work FATF is already doing to overcome the challenges with current information sharing processes. We recommend that FATF evaluate whether these existing private/public information sharing groups can meet the objective set out in 7(b) by including the virtual asset industry.

   Indeed, current information sharing processes under the MLAT and Egmont Group are slow, and a pain point for law enforcement working on cyber investigations. There is a willingness among private sector participants to alleviate these issues and think critically about possible frameworks to share information across borders and weed out illicit activity in the space.

   For example, Global Digital Finance (GDF) proposed a forward-thinking idea in section 2.2 of their input to the FATF public statement. They suggest FIUs could share virtual asset payment addresses of interest to a global network of national FIUs, who, in turn, would issue requests for information to VASPs in their jurisdiction, who would then report back to their national FIU. This would provide a global solution with minimal technical overhead and supervision, and would be capable of operating within existing regulatory frameworks, including data privacy.

Suggestions like GDF section 2.2. should be considered by existing working groups, and the real-time velocity and transparency of virtual asset blockchains would lend itself to initiatives like this.

We appreciate this opportunity to offer comments and look forward to the discussion at the private sector consultation session in Vienna. In the meantime, we are happy to provide further information to support the FATF's work.

**Jonathan Levin**, Co-Founder and COO, Chainalysis
**Jesse Spiro**, Global Head of Policy, Chainalysis