20 April 2021

Comments of Japan Cryptoasset Business Association on the draft revised VASP Guidance

Part I. About the JCBA

The Japan Cryptoasset Business Association (hereinafter referred to as "JCBA," "we" or "us") is a platform for business operators engaged in or considering entering crypto-asset businesses to form human networks, gather their expertise and mutually enhance each other. The purpose of JCBA is to (i) serve as a base for opening up the potential of blockchain technology, which is expected to be a foundation of the self-sustaining and diversified cooperative society to come, and especially crypto-assets, its driving force, (ii) deepen the social understanding of the crypto-asset exchange business and businesses related to crypto-assets and other digital assets on blockchains, (iii) provide an educational environment for persons and organizations who have an interest in crypto-asset businesses, and (iv) aim at the sustainable development of crypto-asset businesses in Japan. JCBA has 100 members, consisting of many VASPs as well as various related business operators such as banks, securities companies, communication service providers, systems companies, law firms, auditing firms and internet media. JCBA is a general incorporated association established in 2016, and has continuously held study sessions regarding the virtual assets, as well as made a number of recommendations regarding Japan's legislation on virtual assets and VASP.

JCBA supports the efforts to achieve soundness of the crypto-asset business through effective AML/CFT measures and appreciates the opportunity to comment on the Draft updated Guidance for a risk-based approach to virtual assets and VASPs published by FATF ("Guidance"). Our opinion is as follows.

Part II. General Comments on the Guidance

1. Significance of Virtual Assets

Virtual asset ("VA") is a digital representation of value that is different from conventional financial instruments and is innovative in that all transactions, including transfers and exchanges, can be conducted on a P2P basis.

With the emergence of VA, individuals who previously had access to financial services only through financial institutions are now able to access financial services directly through P2P transactions. Individuals are able to use financial services such as transfers, exchanges, and loans at lower costs because the various costs involved in the operation of financial institutions are not passed on to them.

This is not only beneficial from the viewpoint of financial inclusion[1], which means that

[1] The Leaders' Declaration of the 2010 G20 Seoul Summit recognized financial inclusion as a key pillar of the global agenda and endorsed a specific Financial Inclusion Action Plan (http://www.g20.utoronto.ca/2010/g20seoul.pdf).

individuals who do not have bank accounts will be able to receive financial services, but also brings great benefits to individuals who do have bank accounts, such as the benefit of lower cost and more efficient financial services.

2. Democratic Legitimacy of Regulations

The VA industry basically agrees that VAs should be regulated according to their characteristics. However, not all regulations can be legitimized solely for the purpose of AML/CFT.

Generally speaking, in order to legitimize a regulation, the procedures therefor must be appropriate and the contents of thereof must be reasonable.

From the viewpoint of procedural appropriateness, it is necessary to present supporting data in the regulatory implementation process, followed by a process for reflecting opinions of stakeholders democratically. In addition, from the viewpoint of reasonableness of the contents of the regulations, it is necessary to carefully examine (i) whether the regulatory objectives are legitimate, (ii) whether the means to achieve the regulatory objectives are reasonable, and (iii) whether the benefits lost by the restrictions on rights and freedoms are appropriately weighed against the benefits to be derived.

In particular, it should be noted that regulations on VAs and P2P transactions have a strong aspect of restricting personal property rights and privacy rights of individual users beyond the industry regulations on financial institutions. For example, if an individual user holds a VA, the user has the right to withdraw the VA from the VASP, and prohibiting it will directly restrict the user's proprietary rights. In situations where the user is suspected of being involved in a crime, withdrawals may be restricted, as in the case of cash, but we believe that the user's rights cannot be restricted in the absence of such reasonable grounds. In addition, attempts to visualize P2P transactions are highly likely to lead to government interference with the privacy of private lives of individuals through their use of funds, as well as interference with the flow of funds in activities related to the freedom of expression, such as lawful demonstrations, news gathering and news reporting. Such interference should not be allowed only for the reason that they engaged in P2P transactions.

In principle, in order to introduce these types of regulations that restrict the rights and freedoms of individuals, it is necessary to hold democratic discussions among elected representatives from the perspective of what regulations are permissible under the legal system of each member country. However, if an arrangement is finalized by FATF, then, despite the fact that such arrangement is not a treaty, the member countries will be forced to introduce regulations consistent therewith through the mechanism of mutual evaluation in order to continue to participate in the international financial network, which leaves little room for discussion by the legislative bodies of each country. Therefore, we believe it is essential for FATF to ensure democratic legitimacy before finalizing an arrangement.

3. Appropriateness of the Regulatory Implementation Process

With regard to the regulatory implementation process, FATF occasionally holds Private Sector Consultative Forum ("PSCF") , which is a forum for hearing the opinion of the

private sector. The introduction of the "travel rule" was discussed on May 6, 2019. During this discussion, there were many voices that opposed the proposed regulation on the ground that they may be effective for traditional financial institutions but not necessarily effective for VAs. Some participants commented that the proposed regulation was "technically possible," but being "technically possible" does not support the reasonableness of regulation. Eventually, the travel rule was finalized mostly as originally proposed in June 2019, but the details of FATF's considerations of the rule based on the discussions at the PSCF have not been disclosed.

In this way, FATF's regulations have been decided upon in closed meetings between relevant authorities, and disclosure has been very limited. Proceedings at the PSCF are not open to the public, and even when public consultation is held, the details of submitted comments and FATF's responses thereto are not made public. It is doubtful whether such procedures can be said to be democratic.

For the proposed revision of the Guidance, we strongly request that FATF disclose the comments submitted in the public consultation and FATF's views thereon, hold a PSCF to hear from a wide range of stakeholders including VASPs, and disclose the minutes of the PSCF as well as the results of FATF's reconsideration based on discussions at the PSCF before finalizing the revision. In addition, we urge FATF to establish a mechanism to reflect the opinions of the private sector on an ongoing basis, such as establishing within FATF a working group consisting of representatives from the private sector and reflecting the opinions of the working group from the drafting stage.

4. Necessity of Clear Regulations

If each jurisdiction enacts legislation based on the FATF Recommendations, license or registration will be necessary for becoming a VASP. If a person acts as a VASP without a license or registration, it is likely that such person will not only be subject to administrative punishment but also be subject to criminal penalties.

Given this, the requirements of the FATF Recommendations and Guidance must be clear. Finalizing ambiguous Guidance is likely to lead to the introduction of ambiguous penal legislation in different jurisdictions. This not only suppresses innovation, but can lead to human rights violations through the application of unclear penal laws. Clarification of penal laws is a constitutional requirement in Japan, and we understand that it is also a constitutional requirement in many FATF member countries.

5. Excessive Regulations Lead to Unintended Consequences

If regulations that cannot be legitimized from the viewpoint of 2. above are introduced, it is highly likely that they will lack effectiveness for new technologies that continue to emerge. As a consequence, the strength of sound VASPs seeking to comply with regulations, which is a key element of AML/CFT measures, may be unduly exhausted or weakened. In addition, VASPs reluctant to comply with regulations may move to less regulated countries, making it difficult for law enforcement authorities to investigate and track transactions.

6. Necessity for Regulatory Authorities to Improve Efficiency through Promotion of Reg Tech, etc.

While a virtual asset transactions are recorded on public blockchain and are thus transparent, the VASP performing KYC is considered to play an important role when identifying the person that conducted the transaction. In the future, inquiries from law enforcement authorities to VASPs may increase more than those to traditional financial institutions, as virtual asset transactions are publicly conducted. However, responses to these inquiries lead to a significant cost and weakening of regulatory compliant VASPs, who play an important role in the investigation process as described above. The current problem is that, even within the same jurisdiction, there are many inquiries in different formats and methods from law enforcement authorities in different regions, and the cost of dealing with them is increasing for VASPs. In addition, in some jurisdictions, VASPs are required to spend a lot of time on work other than the investigative work originally required in connection with the investigation, due to circumstances such as that inquiries are made in traditional, paper-based format or that the web reporting system is user-unfriendly and inefficient. FATF should not only require VASPs to secure resources to cooperate in investigations, but also consider having jurisdictions require investigative authorities to establish efficient methods of inquiry, and encourage review and improvement of such methods (such as standardizing inquiry formats, improving reporting systems, and introducing mechanisms to aggregate inquiries by region), so that VASPs do not have to spend unnecessary resources. We believe that this would facilitate VASPs' responses to inquiries and improve efficiency from the viewpoint of AML/CFT.

Part III. Comments on Individual Paragraphs

1. Paragraph 13 and Paragraph 22

While some countries, including Japan, have implemented strict regulatory regimes for VASPs in accordance with the FATF Recommendations, many jurisdictions have not done so. And, as with the existence of tax havens in taxation regimes, it is clear that VASPs in such jurisdictions have become regulatory security holes. As long as such jurisdictions continue to exist, seeking increased regulations from countries that have already implemented such regulations will likely lead to the unintended consequence that compliant VASPs will lose competitiveness and non-compliant VASPs will earn greater profits. Therefore, we believe that the priority in allocating resources at this point should not be to require countries that have already implemented the regulations to become stricter, but to urge countries that have not implemented the regulations to implement the regulations. We believe that this is essential for the realization of a level playing field, which is a requirement for each country under Paragraph 22 c).

2. Paragraph 16

Although central bank-issued digital currencies are uniformly excluded from application, consideration should be given to the handling of digital currencies in non-FATF member countries and the possibility of central banks issuing assets in arbitrary

digital formats. Even in the case of central bank-issued assets, if the activities conducted are substantially the same as those of VAs, such assets should be treated in the same way as VAs from the viewpoint of a level playing field under Paragraph 22 c).

3. Paragraph 19

Paragraph 19 cites "Virtual Assets Red Flag Indicators of ML/TF" and suggests that "VAs are becoming increasingly mainstream for criminal activity more broadly." However, the report does not include statistical data, and some of the examples presented therein do not include monetary amounts, so there is no evidence from the report that VAs have become mainstream for criminal activity. Rather, a recently published report by the former CIA Director of Intelligence provides a variety of rationales and points out that the "generalizations about the use of Bitcoin in illicit finance are significantly overstated"[2]. A recent report from Chainalysis, a leading blockchain analytics firm, also noted that criminal activity using virtual assets is on the decline, with only 0.34% of all virtual asset transactions in 2020 associated with illicit activity[3]. A September 2020 report commissioned by SWIFT to BAE Systems also noted that the amount of cash laundered in the identified cases of laundering through virtual assets is smaller than those laundered by traditional methods[4].

As this Guidance should be based on certain data and criteria within FATF, such statistical data should be disclosed and presented as links, etc.

4. Paragraphs 21 and 28

It states, "It is important that FIs apply the risk-based approach properly and do not resort to the wholesale termination or exclusion of customer relationships within the VASP sector without an appropriately-targeted risk assessment." In practice, however, due to de-risking by banks, the relationship between banks and VASPs is quite different from such guidance. We believe that it is necessary for the member countries to conduct investigations of actual conditions and take proactive improvement measures.

5. Paragraphs 31, 155 and 167

It is pointed out that "VA products and services that facilitate pseudonymous or anonymity-enhanced transactions … pose higher ML/TF risks." However, there is a growing demand for privacy protection, and it is expected that there will be a social demand for anonymization measures in financial transactions. While it is possible for consumers to trade in cash if they wish to protect their privacy, it seems excessive and disproportionate to deny all anonymous transactions only with respect to VAs.

In such anonymized financial services, it is possible to conduct KYC at the start of

---

[2] Michael Morell "An Analysis of Bitcoin's Use in Illicit Finance" Crypto Council for Innovation, April 6,2021, https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf

[3]"The 2021 Crypto Crime Report" Chainalysis, February 16, 2021, https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets

[4]"New Report Reveals How Cyber Attackers 'Cash out' Following Large-Scale Heists." BAE Systems, September 2, 2020, https://www.baesystems.com/en-financialservices/insights/news/report-reveals-how-cyber-attackers-cash-out-following-heists

transactions as well as risk assessment based on KYC. However, even service providers may find it difficult to implement the travel rule because some of the details of individual transactions are anonymized.

Therefore, the travel rule should not be applied to all transactions. Even in the case of providing anonymous services, it would be possible to take measures for risk mitigation at the VASPs, such as setting a limit on the amount of money that can be handled in anonymous transactions and comprehensively filtering black addresses in the entire service. We believe that transactions should be exempted from application of the travel rule to a certain extent if such risk mitigation measures are taken. Paragraph 167 requires the implementation of the travel rule for transactions below USD/EUR 1,000 as well, but the implementation of the travel rule should not be compulsory if other risk mitigation measures are taken.

6. Paragraphs 35 and 36

As confirmed in Paragraph 34, the FATF Recommendations impose obligations on intermediaries between individuals and the financial system and do not apply to P2P transactions in cash or VAs.

Since VAs, like cash, is originally assumed to be used in P2P transactions, a customer cannot be judged to be suspicious solely by the fact that the customer conducted P2P transaction of VAs. As in the case of using cash, risks should be assessed as high only when, for example, transactions are conducted in unnaturally large amounts or large numbers.

Regarding the last sentence of Paragraph 35, if the purpose is to require VASPs to "provide greater visibility over P2P transactions" through "blockchain analytics" even in P2P transactions in which VASPs are not involved, we believe that this is an excessive demand. We also believe that it is problematic from the viewpoint of protecting privacy to interfere with payment and other activities by customers in their private lives.

It is also pointed out that ML/TF risks "should be addressed in the design or development phase" of VAs, but since the software development activities themselves do not fall under VASP definition, this seems to be outside the scope of the Guidance. We believe that discussions on how to establish standards for the design and development of VAs should be held with multiple participants who actually design VAs, for example, with a focus on ISO.

7. Paragraph 38

FATF defines VA as "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." However, since any digital representation can be an investment target, all digital data can fall under a VA in this definition, which is not effective. The requirements for falling under a VA should be made clearer.

8. Paragraphs 42 and 78

Paragraph 78 suggests that "certain virtual items" are also included in the definition of

VA. However, it should be made clear that non fungible tokens ("NFT") with the following characteristics do not fall under VAs as they are considered to have low risk from the viewpoint of AML/CFT, which is the purpose of FATF:

(i) The transaction history remains on the blockchain;

(ii) The uniqueness of each NFT (the fact that it is easily identifiable); and

(iii) The number of issuance is limited and mass purchase/mass sale is difficult in general.

9. Paragraphs 54 and 55

According to this guidance, service providers that are outsourced by VASPs to provide some of the multisignatures on their behalf may also fall under VASPs. However, VASPs engage such service provider for meaningful purposes such as improving security. In addition, the outsourcer VASP can implement the measures required of VASPs and can also have control over the outsourcee under a service agreement. We believe that it is an excessive regulation to consider such outsourcees as VASPs and that risk mitigation should be promoted by appropriately regulating the VASPs who are the outsourcers.

10. Paragraph 55

According to Paragraph 55, if a service provider has control over some of the private keys for multisignature, such service provider is a VASP even if it needs private keys held by others to perform a transaction.

On this basis, even a service provider of Decentralized Digital Identity, which provides signatures only when the user is unable to recover on his or her own, is uniformly deemed to be a custodian, which would significantly hamper innovation.

The definition of VASP is as described in paragraph 47, and the interpretation of VASP definition should be considered within the meaning of the phrase "safekeeping and/or administration of virtual assets." For example, in the case of a 2-of-3 multisig, a person holding two or more private keys has the authority to transfer a virtual asset, and thus, if such person is holding the private keys on behalf of another person, it will fall under a VASP. On the other hand, a person who has only one private key will not fall under a VASP. According to Paragraph 55, even when the customer is able to transfer the virtual asset independently, the service provider will fall under a VASP if it holds some of the private keys. However, it is apparent that if the virtual asset could be transferred independently of the intention of the service provider, this does not fall under "safekeeping" or "administration." The original text of Paragraph 55 is a rewriting of the definition beyond broad interpretation and should be revised.

According to the definition in the draft Guidance, miners will also be considered as VASPs as all blocks require signatures with the keys held by the miners, which is inconsistent with the interpretation that miners do not fall under VASPs. Whether a person is a custodian should be defined by technical specifications, such as the format of transaction, rather than whether a key is required.

11. Paragraphs 55, 57 to 60, 62, 64, 65, 69, 72, 75, 91 and 178

In these paragraphs, the term "facilitate" extends the scope of regulation in an

ambiguous manner. It is too broad and vague for a person to fall under a VASP only by "facilitating." As the term "facilitate" is not defined in the FATF Glossary, we believe that this term should be deleted. It also seems to be inconsistent with the guidance that a person that provide "ancillary services" does not fall under a VASP.

12. Paragraphs 56 and 57

(1) According to Paragraph 57, "the owner/operator(s) of the DApp likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer." However, the concept of "the owner/operator(s) of the DApp" is ambiguous. If it is unclear what "own" and "operate" specifically mean, it is possible that all persons involved in DApps may fall under VASPs. Also, because smart contracts can be deployed on the public-chain by anyone and such smart contracts can be used by anyone, it is not effective to consider everyone as a VASP.

The individual transactions executed by the decentralized application DApp are performed through smart contracts deployed on the blockchain, and it is not that the "owner/operator" of the DApp executes the transactions for or on behalf of the customer. As with VA transfer transactions between individuals using unhosted wallets, these transactions are regarded as P2P transactions and do not involve any intermediary subject to financial regulations. Paragraph 34 states that P2P transactions are not subject to the FATF Recommendations and we believe that a similar interpretation should apply.

(2) If a DApp is built, for example, as a smart contract on an Ethereum network, the DApp is essentially an unalterable computer program that will continue to run automatically as long as the Ethereum network continues to run. Therefore, the concept of "operate" does not apply. In addition, the concept of "own" is also unlikely to apply because the source codes of DApps can usually be viewed and copied by anyone.

(3) As stated in the draft Guidance, developers and others may also hold certain administrative keys for DApps. Holding such an administrative key is necessary to fix a serious bug in a smart contract when it is found. It is clear that bugs cannot be completely prevented in any software development, and fixing bugs after software is released is a mandatory task for developers. Holding an administrative key to the extent necessary for purposes such as fixing bugs is a part of the development activities, and such fact is not sufficient by itself to consider a developer as a VASP. The same applies to the case where the administrative key is held for upgrading the functions of the DApp. These activities are part of software development and do not constitute VA transactions for or on behalf of the customer. Therefore, as described in Paragraph 68, these do not fall under the definition of VASP.

On the other hand, in cases where the holder is able to access a user's assets with an administrative key or to play a role in the success or failure of individual transactions, the definition of VASP may be applicable.

Based on the above, whether the holder of the administrative key is a VASP should be determined based on whether the holder exchanges or transfers VAs as a business for or

on behalf of the customer, taking into account comprehensively the details of its privilege concerning the administrative key, the conditions for exercising the privilege, the frequency of exercising the privilege and other factors.

(4) Also, even if any portion of the fees paid by the user for the use of the DApp is sent to a specific address, that fact alone does not mean that the holder of the address receiving it conducted a transaction for the user. For example, if the holder of the address does not have any special authority concerning the DApp and does not play a role in the success or failure of the transaction, it cannot be said that the holder falls under the definition of VASP. Although the fact that fees or other benefits have arisen may imply that the recipient thereof has some involvement in the DApp, it should be made clear that such fact is not sufficient by itself to say that the recipient is a VASP.

(5) In view of the above, even if certain persons involved in the DApp beyond the development activities fall under VASPs, it is assumed that the persons involved in the DApp services are very compact entities or individuals. It is practically difficult to identify in advance and regulate all such natural or legal persons, and there is concern that such regulation will hamper innovation and financial inclusion. On the other hand, it is possible to recognize expansion of the scale of DApps, and if the persons involved therein fall under VASPs, regulations should be imposed according to the scale.

In addition, even if a service provider involved in a DApp falls under a VASP, separation of the VASP and the KYC provider should be permitted. This will make it possible to invoke the KYC provider's contract within the DApp's contract and delegate filtering and monitoring to the KYC provider, which is expected to improve effectiveness and efficiency of implementation of the regulations. In such case, a person falling under a VASP would outsource filtering and monitoring work and travel rule compliance work to the KYC provider, and the KYC provider will perform these works.

13. Paragraph 58

With regard to the word "issuance" in Paragraph 58 b), the issuance of a virtual asset itself does not fall under an "exchange" or a "transfer." For example, a person who mines Bitcoins or implements a hard fork of the Bitcoin and grants the forked coins to the Bitcoin holder is involved in the "issuance," but such person cannot be said to have exchanged or transferred the VA in the course of trade on behalf of the customer. It should be clarified under what circumstances services related to the issuance of VAs fall under a VASP.

14. Paragraph 62

It states, "Providing the functions outlined in the definition should be the determining factor rather than a categorization as a lawyer," but as mentioned above, whether a person falls under a VASP is a criterion for determining whether the criminal law of a member country is applicable, and thus should be considered as a legal interpretation. This guidance is not appropriate because it would undermine the "rule of law" and allow

arbitrary interpretation.

In addition, the definition of VASP does not include the phrase “helps/promotes,” and the interpretation that “any provider that helps/promotes customers hold or use their VAs” is a VASP is a rewriting of the definition beyond broad interpretation.

15. Paragraphs 63 and 64

According to Paragraph 63, the definition of VASP may include persons who manage smart contracts to which they are not a party. However, the concept of “control of smart contracts” is ambiguous, and there is concern that it may be applied arbitrarily in different countries.

Smart contracts usually include those that provide services as software and those that are called proxy contracts, which serve as the gateway to access the former type of smart contracts. The reason why they are designed and deployed in such dual structure is to enable emergency response such as separating the subsequent smart contracts from the proxy contract in case of a bug in the code. Therefore, if a developer abandons the authority to update a proxy contract, it will not only have a significant negative impact on users, but may also increase the risk of malicious uses, such as money laundering, as a result of such smart contracts being left unchecked. We believe that the development of a smart contract with appropriate management authority, such as the authority to separate subsequent smart contracts in order to deal with such an emergency, is directly linked to safety. In addition, we believe that it is inappropriate to interpret those who have such privilege as falling under the definition of VASP only based on the fact of granting a certain level of privilege concerning the smart contract.

16. Paragraphs 64 and 65

According to the guidance under these paragraphs, the act of a company developing its own public blockchain could also be considered to be a VASP as “participation in or provision of financial services related to an issuer’s offer and/or sale of a VA”. However, “participation” is not defined and the scope of regulation is vague and broad. The use of the term “facilitate,” which does not exist in the definition of VASP, is also expanding the scope of regulation more vaguely. As stated above, it is necessary to clarify the scope of regulation.

Practically, it would be difficult for any entity to identify every public blockchain user. In addition, overregulation leads to hampering innovation and financial inclusion. As specified in Paragraph 68, developers of the blockchain itself should be excluded from the definition of VASP, even if they are involved in the issuance of VAs. On that basis, it would be sufficient to confirm the applicability of a VASP only with respect to entities that sell or exchange virtual assets to or with the public.

17. Paragraph 74

With regard to “decide whether parties … are VASPs on a functional basis,” it is considered that software development activity does not fall under a VASP even if it enables P2P transactions, just as unhosted wallets do not fall under VASPs. We believe

that the description “only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and issuance will generally not be a VASP” is inconsistent with such interpretation and needs to be revised.

18. Paragraph 75

This paragraph states that most mechanisms that are currently implemented, even those that are categorized as P2P platforms, may have some parties involved with the product at some stage of its development and launch, and such parties are considered as falling under VASPs. However, as entities solely engaged in development and sales activities of the software do not fall under VASPs, this interpretation is overly broad and needs to be revised.

In addition, with regard to the description that “finding services” may “qualify as VASPs even if not interposed in the transaction,” it should be clarified what conditions the “finding services” need to meet in order to qualify as VASPs.

19. The Whole of Paragraph 91

Paragraph 91 encourages the separation of transactions between VASPs and P2P transactions. Such separation has negative aspects such as (i) impediment to financial inclusion, (ii) the risk of destabilizing security of the industry, since the security of VAs relies on the development and operation by the development community of the core part of P2P transactions, and (3) significant restriction of the rights of individual users.

On the other hand, the FATF document “12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS/VASPS” dated June 2020 states that “there was insufficient evidence demonstrating that the number and value of anonymous peer-to-peer transactions has changed enough since June 2019 to present a materially different ML/TF risk” and that “further research could be undertaken.” In the FATF document “FATF Report to G20 on So-called Stablecoins” dated the same month, it is described that so-called stablecoins could pose a significant ML/TF risk if they were to be mass-adopted while, on the other hand, “there is a risk tolerance in the revised FATF Standards for a certain level of anonymous payments”, similar to cash payments. The FATF document “VIRTUAL ASSETS RED FLAG INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING” dated September 2020 makes no reference to P2P transactions. We believe that information should be disclosed on what considerations were made that led to the change in perception after the release of these reports. We also believe that internal statistical estimates, if any, should be made public.

20. Paragraph 91 a)

There is description on the submission of Currency Transaction Reports (CTRs) by VASPs to the authorities in this paragraph. In a traditional fiat currency transaction, the law enforcement authority would not be able to know information about the transaction unless the information is presented in the CTR or the authority makes an inquiry. However, since virtual asset transactions are recorded in the public blockchain, the law enforcement authority is in a position to confirm such information without any report like the CTR.

The aforementioned report by the former CIA Director noted that virtual asset blockchain analysis "is a highly effective crime fighting and intelligence gathering tool" but is "underutilized" by law enforcement and others[5]. It is desirable that the authorities promote Reg Tech and improve efficiency in light of such characteristics of the virtual assets.

21. Paragraph 91 c)

Limitation on transactions with persons using unhosted wallets significantly restricts users' rights and significantly impedes financial inclusion. Even taking into account the objective of reducing ML/FT risk, it seems to be excessive and out of balance with the right and benefits to be lost. Users have a legitimate incentive to use unhosted wallets, such as avoiding leakage of VAs from VASPs, and there is no need to exclude them from transactions only for the reason that they are using unhosted wallets.

22. Paragraph 122

Paragraph 122 states that licensing or registration regulations similar to those for VASPs should be put in place for stablecoins, including algorithmic ones, prior to their launch. However, it is not clear for what reason and at what point the development of the algorithm falls under a VASP. As it is clearly stated in Paragraph 68 that FATF does not regulate the development of software itself, it should be clarified that individual developers of algorithmic stablecoins are not VASPs unless they exchange or manage the virtual assets for or on behalf of the customer.

23. Paragraph 135

At the beginning, it states, "As discussed previously, VAs have certain characteristics that may make them more susceptible to abuse by criminals, money launderers, terrorist financiers, and other illicit actors," but it is not clear which paragraph was quoted. In any case, it should be made clear what consideration has been made that led to such recognition.

The reports by BBC and others in 2020 (https://www.bbc.com/news/uk-54226107) revealed that even the limited documents leaked indicate that suspicious transactions of about USD 2 trillion, which is equivalent to the total market value of VAs, were conducted through financial institutions other than VASPs. It is necessary to reconsider whether it can be said without comparison with such transactions that VAs are particularly susceptible to abuse.

24. Paragraph 152 et seq.

The reasonableness of immediately requiring VASPs to implement the travel rule described in the Guidance is questionable for the following reasons.

First of all, of the contents of the travel rule, the requirement that VASPs obtain information on the originator and the beneficiary of a virtual asset transfer of a certain amount or more basically seems to be reasonable. In such case, VASPs are able to obtain

[5] Michael Morell; please see Note 2 above.

accurate information on their own customers, but information on parties other than their own customers will have to be obtained from their customers on a declaration basis. At present, VASPs only obtain information on their own customers in most cases, so obtaining information on the originator/beneficiary of the transfer will be a substantial progress from the AML/CFT perspective. In addition, obtaining such information on the originator/beneficiary can be dealt with relatively quickly because, although it will be necessary to amend the contracts with customers and to upgrade their systems, it will not be necessary to share personal data with other VASPs.

On the other hand, with regard to the part of the travel rule that require sharing of obtained personal data with other VASPs, there are issues such as that (i) it is necessary to unify the data format of the information to be shared, (ii) there is no common tool for communication that is secure and efficient, (iii) it is difficult to confirm whether the personal data will be properly protected by the VASP to which the transfer is made, and (iv) there is a need to satisfy the regulatory requirements for personal data protection in each country. Overcoming these issues will obviously require time and financial costs, such as those related to the establishment of regulatory framework in each country and the development of common rules and systems agreed to be used by VASPs in each country.

Also, if the VASPs in each country take appropriate AML/CFT measures, the risk of VA transfer between VASPs can be lower than those with non-VASPs. However, sharing of personal data with the counterparty in a transaction with a non-VASP is difficult to do and is not required by this draft Guidance (Paragraph 180). This goes against a risk-based approach. In addition, taking into account the time and cost required for sharing personal data as well as the risk of leakage of personal data, the reasonableness of uniformly requiring the sharing of personal data among VASPs at this point is questionable. Given that both the authorities and the private sector have limited resources and that efficient measures are required to be taken, it would be desirable to first implement as soon as possible the regulations that are considered to be effective, such as obtaining information on the originator/beneficiary and the performance of screening using such information.

25. Paragraph 156

Paragraph 156 states that all VA transfers should be treated as cross-border wire transfers. However, it is clear that when a VA transfer is made, if it is specified that the beneficiary is a VASP within the same country as the originator, it should be treated as a domestic wire transfer. The Guidance should clearly state that VA transfers specified as those within the same country should be treated as domestic wire transfers.

26. Box 4 and Paragraphs 158 to 160

The names, addresses, national identification numbers, customer identification numbers, and dates and places of birth of the originator and the beneficiary are personal information, and the transfer of such information is subject to the privacy regulations in each country. In order to implement the travel rule, it is necessary to introduce uniform laws and regulations concerning the transfer of personal information across countries.

27. Paragraph 167

Paragraph 167 states that (i) the name of the originator and the beneficiary and (ii) the wallet address should be collected even for VA transfers of less than USD 1,000.

At present, privacy is maintained for cash settlements in daily life, but the use of cash tends to be decreasing. As a result, personal privacy is becoming more limited. Crypto-currencies that are developed and operated open-source are currently the only electronic currencies that have the potential to be trusted by citizens to be technology that indeed preserves privacy. Furthermore, the self-sovereign crypto-currencies are expected to be the foundational layer of the Internet, similar to TCP/IP. Based on the above, we believe that measures should be taken such as setting a specific threshold and exempting the information collection obligation concerning (i) and (ii) above, as in the case of cash, if the total daily amount used is below the threshold[6]. If such measures are not approved, the details of the rationale therefor should be clarified because it will severely restrict the right of privacy of individuals.

In addition, among VA applications, micro-earning applications, which repeat the transfer of a very small amount (for example, 1 cent) to the same person in the same application, is increasing. In such case, we believe that it should be allowed, for example, to set the maximum daily total amount and record (i) the name of the originator and the beneficiary and (ii) the wallet address by treating multiple transfers as a single transfer if the total amount reaches a certain amount.

28. Paragraph 176

It states, "Regardless of the lack of regulation in the beneficiary jurisdiction, originating entities can require travel rule compliance from beneficiaries by contract or business practice," but such contractual/business practice does not exist at this time and are not realistic. In order to ensure the uniformity of regulations for VAs and VASPs, it is necessary to establish international uniform commercial transaction rules in accordance with actual conditions when implementing the travel rule.

29. Paragraph 179

Paragraph 179 provides that consideration should be given to requiring VA transfers to and from unhosted wallets to be treated as "higher risk transactions that require greater scrutiny and limitations." However, as described above, users have a legitimate incentive to use unhosted wallets, such as avoiding leakage of VAs from VASPs, and there is no need to exclude them from transactions only for the reason that they are using unhosted wallets.

30. Paragraphs 246 and 252

Paragraph 246 requires that VASPs not carry out transactions if they cannot apply the

[6] As previously mentioned, the "FATF Report to G20 on So-called Stablecoins" also states, "Similar to other forms of payment (such as cash), there is a risk tolerance in the revised FATF Standards for a certain level of anonymous payments for virtual assets."

appropriate level of CDD. On the other hand, the Guidance generally provides that (i) most of the service providers involved in VAs are VASPs, and (ii) transactions with self-hosted wallets have a high risk. As a result, it is expected that small transactions from developed countries to persons in developing countries who do not have IDs will become almost impossible. Although there is a relationship of trade-off between financial inclusion and AML/CFT, very small transactions such as those of less than USD 1 a day have a low risk and thus should be permitted even if CDD is not fully performed (even with simple ID verification).

End