King & Spalding

Client Alert

Providing Strategic Legal Guidance to the Global Financial Services Industry

FINANCIAL SERVICES

APRIL 9, 2021

For more information, contact:

Jeffrey Telep
+1 202 626 2390
jtelep@kslaw.com

Shaswat Das
+1 202 626 9258
sdas@kslaw.com

A. Seth Atkisson
+1 202 626 9257
satkisson@kslaw.com

Adam Harper
+1 202 393 3799
arharper@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

FATF Releases Proposed Updates to Cryptocurrency Regulation Guidance

On March 19, 2021, the Financial Action Task Force ("FATF"), an intergovernmental body tasked with setting international standards aimed at preventing money laundering and terrorist financing ("FATF Standards"), released its Draft Updated Guidance For a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (the "Guidance"), which is an update to guidance released in 2019. The 2019 guidance was released to help clarify the anti-money laundering ("AML") and counter-foreign terrorism ("CFT") financial obligations of countries and Virtual Asset Service Providers ("VASPs") under the FATF Standards. If ultimately adopted by FATF, the Guidance will constitute recommendations on how to supervise and regulate virtual assets ("VAs") and VASPs. The more than 200 countries and jurisdictions that are members of FATF may then adopt and implement the recommendations. FATF has invited public comment, especially from the "VA community, including academics and policy bodies, VASPs, technology developers and providers (particularly in relation to the travel rule), [and] other regulated entities (such as banks)," on the Guidance. Comments to FATF concerning the Guidance must be received by April 20, 2021 (18:00 UTC).

The updates to the Guidance concern six main areas:

- Expanding the definitions for what constitutes a VA and a VASP;
- How FATF Standards apply to stablecoins;
- Additional guidance about risk and risk mitigation for peer-to-peer transactions;
- Updated guidance about the licensing and registration of VASPs;
- Additional guidance about the "travel rule"; and
- Fostering information sharing and co-operation between VASP supervisors (*i.e.*, regulators).

EXPANDED DEFINITIONS OF VAS AND VASPS

The Guidance was updated to state that the definitions of VA and VASP are to be interpreted and read "broadly." The Guidance states that the focus of what constitutes a VA is "the basic characteristics of the asset, not the technology it employs." According to the Guidance, VAs "must be digital, and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes." Although FATF does not intend for an asset to be both a VA and a traditional financial asset, it concedes that some assets may be classified differently in various jurisdictions depending on a jurisdiction's adopted framework. When determining whether to classify an asset as a VA or a traditional financial asset, the Guidance advises jurisdictions to consider the classifications best suited to mitigating and managing the risk of the assets under their regulatory system and the commonly accepted usage of the asset.

As with VAs, the Guidance states that jurisdictions should not determine whether an entity is a VASP based on the technology it uses or the label that the entity applies to itself. Instead, jurisdictions should look to the specific financial services the entity offers or facilitates, without regard for the "entity's operational model, technological tools, ledger design, or any other operating feature." Importantly, FATF "envisions very few VA arrangements will form and operate without a VASP involved at some stage if countries apply the definition correctly."

The Guidance provides an extensive explanation of the five activities that establish an entity as a VASP, including making it clear that some actors in the cryptocurrency economy previously thought to not be VASPs are within the definition of a VASP. Under the Guidance, a VASP is any natural or legal person who is not covered elsewhere in the Guidance and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;

ii. Exchange between one or more forms of virtual assets;

iii. Transfer of virtual assets;

iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or

v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Regarding items (i)-(iii), the Guidance states that the entity does not need to provide "every element of the exchange or transfer in order to qualify as a VASP, so long as it undertakes the exchange activity as a business on behalf of another natural or legal person." As a result of this expanded definition of a VASP, the Guidance states that the owners or operators of decentralized or distributed applications ("DApps") are likely VASPs because they conduct exchanges or transfers on behalf of their customers, "even if other parties play a role in the service or portions of the process are automated." In addition, the Guidance states that the following entities may also fall within the definition of a VASP: (1) VA escrow services; (2) brokerage services that facilitate the issuance and trading of VAs; (3) order-book exchange services; (4) advanced trading services; (5) VA exchanges or VA transfer services; and (6) kiosk providers.

Furthermore, the Guidance states that "safekeeping" and "administration" should be read broadly and that any entity that "provides or facilitates control of assets or governs their use may" fall within the "conceptual meaning of the words 'administration' and 'safekeeping'." The Guidance offers a custodial wallet service provider as an example of a VASP engaged in safekeeping and/or administration because "they hold and/or keep VAs on behalf of customers."

Finally, the Guidance states that participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset include both financial services provided by the issuer of a VA "as well as services provided by a VASP affiliated or unaffiliated with the issuer in the context of issuance, offer, sale, distribution, ongoing market circulation and trading of a VA (*e.g.*, including book building, underwriting, market making, etc.)."

HOW FATF STANDARDS APPLY TO STABLECOINS

The Guidance reaffirms FATF's previous statement that stablecoins are covered by FATF's Standards, whether as a traditional financial asset or as a VA. In addition, the Guidance states that entities involved in stablecoin arrangements may have AML and CFT obligations. In particular, the Guidance focuses on any central developer or governance body for stablecoins who may establish the rules governing the stablecoin arrangement, manage the stabilization function of the stablecoin, or manage the integration of the stablecoin into telecommunication platforms. These central bodies are especially likely to be considered VASPs if they carry out "multiple functions in the so-called stablecoin arrangement (such as managing the stabilization function)." If there are multiple entities with decision-making authority that can affect the inherent value of the stablecoin, then, depending on their level of influence, each decision-maker also may likely be considered a VASP.

ADDITIONAL GUIDANCE ABOUT RISK AND RISK MITIGATION FOR PEER-TO-PEER TRANSACTIONS

The Guidance affirms that peer-to-peer ("P2P") transactions are not subject to FATF AML/CFT obligations because FATF generally places obligations "on intermediaries between individuals and the financial system, rather than on individuals themselves with some exceptions." As a result, the Guidance states that P2P transactions could pose heightened money laundering or terrorist funding risks, especially if they became more widespread and mainstream. In response to this potential risk, the Guidance offers measures that jurisdictions could undertake, including measures to increase transparency into P2P transactions, limit the availability of certain P2P transactions, and enhance communication with the private sector to assess and understand the risk of P2P transactions.

UPDATED GUIDANCE ABOUT THE LICENSING AND REGISTRATION OF VASPS

The Guidance provides updates about two essential questions related to the regulation of VASPs: (1) which VASPs should be licensed or registered; and (2) how to identify VASPs for licensing or registration. In addition, the Guidance describes certain considerations for licensing or registering VASPs.

- **Which VASPs should be licensed or registered:** The Guidance suggests that, in addition to where a VASP was created and is located, VASPs should be required to be registered or licensed in any jurisdiction where it offers products or services or conducts operations.
- **Identifying VASPs for licensing or registration:** The Guidance states that jurisdictions should monitor for entities engaged in unlicensed or unregistered VA activities, including the creation of an authority responsible for identifying and sanctioning unlicensed or unregistered activity. The Guidance provides six potential investigative tools that could be used to identify unlicensed or unregistered VA activity: (1) blockchain or distributed ledger analytics tools; (2) web-scraping and open-source information to identify online advertising or possible solicitations; (3) information from the general public and industry circles; (4) financial intelligence units or other information from reporting institutions; (5) non-publicly available information, such as whether the entity previously applied for a license or registration or had its license or registration withdrawn; and (6) law enforcement and intelligence reports.
- **Considerations for licensing or registering VASPs**: The Guidance provides additional considerations for jurisdictions to assess license or registration submissions, including administrative considerations (*e.g.*, how to handle a large influx of registration or licensing requests) and more substantive pre-licensing or pre-registration requirements. Some of the Guidance's suggestions include imposing certain staffing or oversight requirements on VASPs before

granting a registration or license (*e.g.*, requiring a resident executive director, specific financial requirements, or compliance policies). The Guidance also suggests requiring that AML/CFT mitigations be built into the products and services "before they are brought to market, as it is much more difficult to do so later." Importantly, the Guidance also suggests that jurisdictions may designate VASPs from jurisdictions with no licensing or registration requirements as "high risk customers or counter-parties," which may trigger additional reporting requirements for VASPs who transact with them.

ADDITIONAL GUIDANCE ABOUT THE "TRAVEL RULE"

The Guidance also revisits the "travel rule", with regard to its application to VASPs conducting domestic and cross-border transfers of VA.

- **Expanded application:** Under the expanded definition of VASPs described above, the travel rule would apply to more transactions involving VAs because more entities would be considered VASPs (*e.g.*, DApps operators). The requirements of the travel rule described in the Guidance include an obligation to obtain certain specified information about the originator and the beneficiary of a VA transaction, submit that information to the beneficiary institution of the transaction, and hold that information. The Guidance provides that jurisdictions may set up a *de minimis* threshold under which the information would not need to be collected.
- **Sanctions screening:** Under the Guidance's revised travel rule, VASPs would also be required to conduct sanctions screening on their customers and the information transmitted as part of the VA transactions.
- **Due diligence:** The Guidance's revised travel rule also states that VASPs should be required to conduct certain due diligence on VA transactions with other VASPs and non-VASPs. For transactions with other VASPs, the Guidance suggests that each VASP conduct periodic due diligence on its counterparty VASP, unless there is something that would indicate a more pressing need for due diligence (*e.g.*, suspicious transaction history). The Guidance notes that "VASPs have customer due diligence obligations at the time of onboarding and on an ongoing basis . . . ." For non-VASPs (*e.g.*, unhosted wallets), the Guidance states that VASPs should be required to treat these transactions as "higher risk transactions" with enhanced scrutiny and limitations. Further, when dealing with non-VASPs, the Guidance would still require VASPs to collect the relevant originator and beneficiary information from their own customer.

INFORMATION SHARING AND COOPERATION BETWEEN VASP SUPERVISORS

The Guidance section outlining FATF's principles of information-sharing and cooperation provides an outline of how VASP supervisors can cooperate to solve shared problems.

- **Identification of Supervisors and VASPs:** The Guidance states that VASP supervisors, and the mechanism to receive communications from other VASP supervisors, should both be clearly identified to foster information sharing and cooperation.
- **Information Exchange:** The Guidance states that certain measures should be undertaken to ensure that supervisors from different jurisdictions can exchange relevant information, including by having an "adequate legal basis" for information sharing, not placing undue restrictions on the sharing of information, and acknowledging the receipt of requests from other VASP supervisors.
- **Cooperation:** The Guidance encourages the use of a single primary supervisor to act "as a focal point through which to coordinate information sharing and cooperation," but also says that the appointment of a primary supervisor is not required. Further, the Guidance states that foreign VASP supervisors should be able "to conduct queries on behalf of

foreign [s]upervisors, and exchange with these foreign [s]upervisors all information that they would be able to obtain if such queries were carried out domestically."

REQUEST FOR COMMENTS

FATF is seeking comments from the public, especially the "VA community, including academics and policy bodies, VASPs, technology developers and providers (particularly in relation to the travel rule), [and] other regulated entities (such as banks)," about the updated Guidance. The central areas of focus for the comments are the following:

1. Does the revised Guidance on the definition of VASP (paragraphs 47-79) provide more clarity on which businesses are undertaking VASP activities and are subject to the FATF Standards?
   a. Is further guidance needed on how the FATF Standards apply to various business models, as stated in paragraphs 56-59? How should the Guidance further address the challenges in applying the definition of VASP to businesses which decentralize their operations across multiple parties?
   b. Is more guidance necessary on the phrase "for or on behalf of another natural or legal person" in the FATF definition of VASP? What are the challenges associated with applying the business-customer relationship concept in the VASP context?
   c. Do the clarifications on the "expansive" approach to the definition of VASP in identifying and policing the "regulatory perimeter" for VASPs provide countries and the private sector with enough guidance? What additional clarity can be given to make the perimeter clearer?
2. What are the most effective ways to mitigate the money laundering and terrorist financing (ML/TF) risks relating to peer-to-peer transactions (*i.e.*, VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets) (see paragraphs 34-35 and 91-93)?
   a. How are peer-to-peer transactions being used for ML/TF purposes and what options are available to identify how peer-to-peer transactions are being used? What role and implications (*e.g.*, benefits) do peer-to-peer transactions and unhosted wallets have in VA ecosystems?
   b. What specific options are available to countries and VASPs to mitigate the ML/TF risks posed by peer-to-peer transactions?
   c. Are the risk mitigation measures proposed in the Guidance in paragraphs 91-93 appropriate, sufficient and feasible?
3. Does the revised Guidance in relation to the travel rule need further clarity (paragraphs 152-180 and 256-267)?
   a. Are there issues relating to the travel rule where further guidance is needed? If so, where? Please provide any concrete proposals.
   b. Does the description of counterparty VASP due diligence clarify expectations, while remaining technology neutral and not prescribing how VASPs must undertake this process (see paragraphs 172-177 and 261-265)?
4. Does the revised Guidance provide clear instruction on how FATF Standards apply to so-called stablecoins and related entities (see Boxes 1 and 4 and paragraphs 72-73, 122 and 224)?
   a. Is the revised Guidance sufficient to mitigate the potential risks of so-called stablecoins, including the risks relating to peer-to-peer transactions?
   b. Are there any further comments and specific proposals to make the revised Guidance more useful to promote the effective implementation of FATF Standards?

CONCLUSION

The updates to the Guidance, if adopted and implemented by the members of FATF, will result in a number of significant changes to the regulation and governance of the cryptocurrency market, such as the expansion of the definition of VASPs to include entities involved with decentralized apps and the increased due diligence expected of VASPs that engage with unhosted wallets. Interested parties should carefully review the updates, determine the potential impacts of the updates to their business, and take advantage of FATF's request for comments on the updates.