November 11, 2021

Skadden

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

This is the second in a series of articles in which we discuss recent efforts by U.S. regulators and other bodies to set expectations and standards with respect to cryptocurrencies and other virtual assets and the impact of these efforts on businesses engaged in virtual asset activities. Read the full series.

FATF Updates Its Global Guidelines for the Regulation of Virtual Assets With an Eye to Emerging Technologies

On October 28, 2021, the Financial Action Task Force (FATF), the international body that sets standards for anti-money laundering and countering the financing of terrorism (AML/CFT), released updated guidance addressing the compliance risks related to virtual assets.

The Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (Guidance) is intended to help government authorities develop regulatory responses to virtual assets (VAs), including cryptocurrencies, and virtual asset service providers (VASPs). It will also help those engaged in VA activities to better understand their exposure to money-laundering and terrorism financing risks and how to fulfill their compliance obligations.

Key takeaways:

- The Guidance explains how FAFT's Standards (FATF Standards), which apply to financial institutions generally, apply to VA activities and VASPs.
- FATF takes a technology-neutral approach to calibrating AML/CFT risks. It seeks to create a level playing field where those offering functionally equivalent products and services are subject to the same risk-based standards, regardless of the underlying technology or the jurisdictions in which they operate.
- The definitions of VA and VASP should be construed broadly, and the Guidance applies these terms to certain novel VA technologies and products, as well as entities that deal in them.
- It sets forth considerations relevant to the licensing and registration of VASPs and examines the tools available to address risks posed by peer-to-peer VA transactions and decentralized finance arrangements.
- It provides additional guidance regarding the implementation of the so-called "Travel Rule" that requires financial institutions to convey important identifying information about parties sending or receiving wire transfers.

- It establishes principles of information sharing and cooperation between government authorities.

While the FAFT has no authority to create direct legal obligations, its Guidance will inform national-level policymaking and encourage the implementation of new laws and regulations. Actors in the VA sphere should pay close attention to the ways in which the Guidance applies to their operations and business models and stay abreast of regulatory developments in the jurisdictions in which they operate as governments worldwide continue to bring their local standards and laws in line with the Guidance.

I. Application of the Definition of VA to Emerging Technologies

A "virtual asset" continues to be defined as a "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes," the definition adopted in the first version of the Guidance in 2019. The Guidance also reiterates that the definition should be broadly construed by government authorities in implementing the FATF Standards. The definition is intended to be technology-neutral and objectives-based — that is, its application should not be affected by the technology supporting the asset in question. The definition is intended to be sufficiently flexible that government authorities can apply it to both existing and emerging technologies.

The latest Guidance does, however, discuss whether certain specific asset types come within the scope of the Guidance and the FATF Standards, explaining that a crucial consideration is whether the asset has inherent value to be traded or transferred and used for payment or investment, or if the asset is merely a means of recording or representing ownership of something else. For instance, while a bank record could be considered a "digital representation of value," the record itself cannot be digitally traded and has no utility as a mode of payment or investment.

Three specific categories of assets discussed are:

A. Central bank digital currencies

The FATF considers central bank digital currencies (CBDCs) to be digital representations of central bank-issued fiat currency, which is already subject to FATF Standards. Accordingly, FATF does not treat CBDCs as VAs for purposes of the Guidance. The Guidance points out, however, that CBDCs may present different or higher AML/CFT risks than standard fiat currencies in light of their digitization, which should be addressed prior to their issuance by central banks and private-sector stakeholders poised to deal in CBDCs.

B. Stablecoins

Stablecoins (cryptocurrencies backed by and intended to track the value of fiat currencies) should be considered either VAs or other financial assets subject to the FATF Standards, depending on the exact nature of the asset, according to the Guidance, a position also outlined in a report by the FAFT to the G20 in June 2020. It highlights that, while stablecoins share many of the same AML/CFT risk factors as other VAs, they have the potential for mass adoption. The relatively stable value of stablecoins compared to the wide fluctuations in value for other cryptocurrencies such as bitcoin could potentially "overcome factors which have held back the widespread adoption of VAs as a means of payment," the Guidance states. Stablecoins could become more widely used to make payment or transfer funds, "particularly where they are sponsored by large technology, telecommunications or financial firms that could offer global payment arrangements."

The Guidance reviews the range of entities that are typically involved in stablecoin arrangements, including central developers or governance bodies, which establish, or facilitate the establishment of, the rules governing stablecoin arrangements. A central developer or governance body would typically be considered a VASP, as would exchangers or custodial wallet servicers that provide services in connection with stablecoin arrangements. To the extent a VASP can be identified within a stablecoin arrangement, the Guidance indicates that government authorities should ensure the VASP implements appropriate controls to mitigate AML/CFT risks. These controls may take a form similar to those the Guidance sets forth with respect to peer-to-peer transactions generally, which are described below in Section III.

C. Nonfungible Tokens

The Guidance defines a nonfungible token (NFT, or "crypto-collectible") as a digital asset that is unique, rather than interchangeable, and that in practice is used as a collectible rather than a payment or investment instrument. Thus NFTs will generally not be considered VAs, though the Guidance stresses that government authorities must consider the nature of the asset and its function in practice when evaluating whether it should be subject to AML/CFT regulation, not the terminology or marketing language that is used to describe the asset. For example, an NFT used for payment or investment purposes, or an NFT that is a digital representation of another (*i.e.*, non-virtual) asset, could be subject to the FATF Standards.

II. VASP Licensing and Registration Considerations

In addition to addressing what constitutes a VA for purposes of the FATF Standards, the Guidance also explores the definition of a VASP. It is defined as "any natural or legal person who is not covered elsewhere under the Recommendations 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 instrument 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."

As described in Section III below, government authorities typically impose AML/CFT obligations on financial intermediaries rather than individual consumers. The identification of a VASP, the catch-all term for financial intermediaries in the VA context, is therefore crucial to establishing the regulatory perimeter around the VA industry. The Guidance acknowledges that jurisdictions are grappling with whether to try to fit VAs and VASPs into existing regulatory regimes or craft new, purpose-built frameworks.

The broad definition of VASP in the Guidance reflects the wide net that the FATF recommends supervisory authorities cast when defining who is subject to AML/CFT regulation. Indeed, the Guidance states that FATF expects that there would be "very few VA arrangements without VASPs involved at some stage if countries apply the definitions correctly." To this end, FATF advises countries to "take particular care to assess any claims that businesses may make as to models of decentralization or distributed services," and to "conduct their own assessment of the business model in line with its risk and their ability to mitigate these risks."

The Guidance does cite some roles that might fall outside the broad definition. Merely issuing a VA, without more, does not constitute the provision of financial services relating to an issuer's offer or sale, the Guidance states. However, such persons may also be providing exchange or transfer services in connection the issuance, which would make the person a VASP under one of the other of the prongs listed above, the Guidance notes. Similarly, it states that creating software to issue a VA does not make the creator a VASP, unless the creator also performs one or more of the covered activities.

The Guidance articulates factors for government authorities to consider in identifying VASPs that should be subject to licensure or registration and where VASPs that operate across several jurisdictions should be licensed or registered. Additional issues flagged include whether to require VASPs to implement AML/CFT programs prior to launch, and whether to apply heightened scrutiny for certain VASPs, such as those located in jurisdictions without effective licensing regimes or those proposing to offer services involving stablecoins or other higher-risk VAs.

The Guidance emphasizes the importance of coordination between government authorities with respect to sharing information on the VASPs operating in their jurisdictions, particularly when it comes to identifying VASPs that may be operating without a license. That coordination is discussed below in Section VI.

III. Peer-to-Peer Transactions

The Guidance defines a peer-to-peer (P2P) transaction as a VA transfer "conducted without the use or involvement of a VASP or other obliged entity (*e.g.*, VA transfers between two unhosted wallets whose users are acting on their own behalf)." As a general matter, P2P transactions that fit within this definition are not directly subject to AML/CFT controls under previous iterations of the FATF Standards, nor are they covered by national AML/CFT laws and regulations, because those typically apply only to financial intermediaries and not individual users or consumers.

The Guidance recognizes the risks posed by P2P transactions, which can occur outside of a jurisdiction's AML/CFT control framework. These risks are mitigated to some extent because there is a publicly available record of all blockchain transactions. The Guidance stresses the need for government authorities to review and understand the degree of AML/CFT risk presented by P2P transactions. It recommends that government authorities conduct outreach to the private sector, particularly VASPs and representatives from the P2P sector; train supervisory, financial intelligence units and law enforcement personnel on the nature of P2P transactional risk; and encourage the development of tools like blockchain intelligence and analytics to collect and assess P2P market metrics and risk mitigation solutions.

The Guidance makes a number of recommendations to mitigate risks associated with P2P transactions, including:

- potentially implementing regulatory controls to increase the visibility of P2P activity;
- ongoing risk-based supervision of VASPs and entities operating in the VA space, particularly those that transact with unhosted wallets;
- restricting the ability of VASPs to facilitate transactions from unknown or unacceptable sources;

- imposing additional requirements (*e.g.*, enhanced record-keeping requirements) on VASPs that permit transactions with unhosted wallets; and
- requiring that VASPs only facilitate transactions with other VASPs or entities subject to AML/CFT requirements.

The Guidance cautions that self-described P2P platforms should be evaluated based on the underlying activity and not on the label or business model ascribed to the platform, and that entities or individuals that provide "matching" or "finding" services to facilitate P2P transactions may be considered VASPs, even if they do not act as intermediaries to the transaction.

IV. Decentralized Finance

A decentralized or distributed application (DApp) refers to a software program that operates on a blockchain or similar technology. DApps can facilitate or conduct the exchange or transfer of VAs. Decentralized finance (DeFi) is used in the Guidance to refer to DApps that offer financial services, such as those offered by VASPs.

The Guidance makes clear that a DeFi application is not, itself, a VASP under the FATF Standards because the standards do not apply to underlying software or technology. As with P2P services, however, self-identification as a DeFi project is not, nor is the nature of the technology involved, dispositive of whether or not the owner or operator of a DeFi arrangement is a VASP. The Guidance notes that "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements . . . may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services."

Owners or operators can be distinguished from other persons involved in a DeFi arrangement based on their ability to control or influence the application's service protocol or underlying assets involved. Such control or influence could take the form of influence over the assets involved in the DeFi arrangement or over aspects of a DApp's protocol, an ongoing business relationship with users or the ability to profit from or set or change parameters of the service.

While the Guidance recommends that the definition of VASP be interpreted broadly, the FAFT acknowledges that there may be cases where no centralized party can be identified in connection with a DeFi application, and thus there is no central owner or operator that meets the definition of a VASP.

The Guidance encourages countries to monitor the risks posed by such DeFi services or arrangements and engage with representatives of the DeFi community. The Guidance suggests that government authorities consider options to mitigate these risks, such as affirmatively requiring that a regulated VASP be involved in any DeFi arrangement or implementing mitigation measures similar to those for P2P arrangements.

V. Continued Focus on Challenges of Travel Rule Compliance in the VA Industry

The Guidance devotes several paragraphs to the application of FATF Recommendation 16 of the FATF Standards to VAs and VASPs.

Recommendation 16 and the Interpretive Note to Recommendation 16 (INR 16) require that regulated entities collect identifying information regarding the originators and beneficiaries of domestic and cross-border wire transfers and transmit that information along the flow of funds to intermediary and receiving financial institutions (FIs). This is known as the Travel Rule. The required information includes the names, account numbers and physical addresses of the originator and beneficiary. The goal is to ensure that institutions establish an appropriate audit trail for qualifying funds transfers and enable FIs to apply their AML and other relevant controls to such transfers.

The Guidance reiterates the FATF's position that the requirements of Recommendation 16 apply to VASPs whenever their transactions, whether denominated in fiat currency or VA, meet the *de minimis* threshold for Travel Rule obligations, which INR 16 suggests be set no higher than $1,000 or €1,000.

Where a VASP or FI is involved on only one side of the transfer (*e.g.*, where the transfer involves one non-custodial, or unhosted, wallet), the Guidance recommends that countries nonetheless require that VASP or FI to adhere to the requirements of the Travel Rule. The Guidance clarifies that FATF does not expect VASPs and FIs originating VA transfers to send the required Travel Rule information to the owner of the unhosted wallet. However, the VASP or FI sending or receiving the transfer should still collect the required information on the transfer from its customer for the VASP's or FI's own recordkeeping purposes.

While the requirements of Recommendation 16 and INR 16 are relatively straightforward in the fiat currency context, significant challenges have emerged in the VA context. These challenges include identifying whether the counterparty of a transaction is a VASP and establishing a mechanism to share Travel Rule information between VASPs in light of the fact that the blockchain does not provide an information sharing protocol for such information.

The Guidance offers several recommendations directed at these challenges. For one, it suggests that VASPs should conduct appropriate due diligence to identify counterparty VASPs, though the Guidance acknowledges that there is currently no

"technically proven means of identifying the VASP that manages the beneficiary wallet exhaustively, precisely, and accurately in all circumstances and from the VA address alone."

There are several third-party solutions in various stages of development or implementation that may enable the more reliable detection of transactions with a counterparty VASP, based primarily on various means of blockchain intelligence or analytics. The success of these solutions may depend on their wide adoption by VASPs so that a network of VASPs can readily identify one another and facilitate the secure transfer of required information. The Guidance urges government authorities to engage and cooperate with each other and the private sector on potential applications and solutions for Travel Rule compliance.

The Guidance also recommends that, once a VASP identifies a counterparty VASP for a given transfer, the originating VASP should obtain and, as necessary, verify relevant identifying and compliance-related information on the counterparty VASP directly from the VASP itself, including the counterparty VASP's ownership information. This would enable a VASP to assess the counterparty VASP's AML/CFT risk profile and the counterparty's controls for managing such risk. The assessment may involve reviewing the counterparty's AML/CFT systems and controls framework and confirming that the counterparty is subject to independent audit. The Guidance cautions that VASPs should complete this assessment before engaging in the transfer of funds or the transfer of Travel Rule information.[1]

The Guidance also stresses that Travel Rule information should only be transmitted to a counterparty VASP in a secure manner, so as to protect the user information against unauthorized disclosure. Moreover, the required information should be transmitted prior to, simultaneously or concurrently with the funds transfer, and may be transmitted through a transfer protocol separate from the funds transfer protocol.

VI. Information Sharing and Cooperation Among Countries Implementing AML/CFT Regimes for VAs and VASPs

In the final section of the Guidance, FATF outlines principles of information sharing and cooperation among government authorities charged with the regulation and supervision of VAs and VASPs. The aim is to: (i) provide a common understanding of the types of information that will be useful to share and when to share it; (ii) outline possible triggers for proactive information sharing or information sharing requests; (iii) establish methods of information sharing; (iv) suggest possible guidelines for authorities when dealing with VASPs in other jurisdictions that do not have sophisticated VA regulatory frameworks; and (v) identify best practices regarding the information countries should maintain on VASPs operating in their jurisdictions.

The Guidance recommends that: (i) regulators not deny information requests from international counterparties on the basis of local data privacy or banking secrecy laws, the existence of ongoing investigations or the nature of the requesting counterparty; (ii) information should only be used for the purpose for which it was sought or provided; (iii) regulators should communicate material emerging issues and developments with other regulators in a timely fashion; and (iv) regulators should cooperate in the most efficient way possible, whether that is on a bilateral basis or a multilateral basis.

VII. Conclusion

The Guidance reflect some key, central themes: (i) an emphasis on substance over form when it comes to identifying VAs and VASPs that may be subject to AML/CFT regulatory requirements; (ii) a focus on cultivating forward-looking regulatory regimes that are nimble and can adapt easily to emerging technologies; and (iii) the importance of information sharing and cooperation among government authorities to create an effective global AML/CFT framework.

Although the Guidance does not create direct regulatory obligations, its recommendations should be viewed, at a minimum, as the common baseline from which the governments of the FATF member countries will operate when applying AML/CFT laws and regulations to VAs and VASPs. Financial institutions and other entities involved in VA activities should therefore examine their existing AML/CFT controls to see if there are opportunities to enhance them in line with the Guidance.

[1] Paragraph 197 of the Guidance provides a flowchart that outlines the proposed steps in counterparty VASP identification and diligence process.

Recent Developments in the Regulation of Cryptocurrencies and Other Virtual Assets

Contacts

Jamie L. Boucher
Partner / Washington, D.C.
202.371.7369
jamie.boucher@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Bao Nguyen
Partner / Washington, D.C.
202.371.7160
bao.nguyen@skadden.com

Khalil Maalouf
Counsel / Washington, D.C.
202.371.7711
khalil.maalouf@skadden.com

James E. Perry
Associate / Washington, D.C.
202.371.7652
james.e.perry@skadden.com

Greg Seidner
Associate / Washington, D.C.
202.371.7014
greg.seidner@skadden.com