Davis Polk

# Financial Action Task Force issues updated guidance for virtual assets

November 1, 2021 | Client Update | 14-minute read

The Financial Action Task Force released an updated version of its guidance on the application of its recommendations to virtual assets and virtual asset service providers on October 28, 2021. The highly anticipated, updated guidance includes recommendations related to stablecoins, non-fungible tokens and decentralized finance.

The Financial Action Task Force (FATF), the inter-governmental body that recommends international standards for anti-money laundering (AML) and countering the financing of terrorism (CFT), released an updated version of its guidance on the application of FATF's recommendations to virtual assets and virtual asset service providers (VASPs) on October 28, 2021 (the Guidance). The Guidance builds on FATF's efforts to apply its AML/CFT framework to the virtual assets industry. United States Treasury Secretary Janet Yellen praised the Guidance, stating, "[t]he United States welcomes the significant work by the FATF to … provide clear standards and guidance for the virtual asset industry. The FATF's work will continue to strengthen global action against illicit finance." Although the measures recommended in the Guidance are not legally binding on FATF members, nor on VASPs directly, the U.S. Treasury Department responded positively to the updated Guidance, and the United States is a co-chair of the FATF body that drafted the revisions.[1]

Since its inception in 1989, FATF has issued 40 recommendations on money laundering (the Recommendations)[2] which, together with the associated guidance, outline the AML/CFT measures that FATF recommends countries implement (FATF Standards).[3] For the most part, the Guidance, if implemented by national regulators, would not introduce new requirements for the VASPs. Rather it clarifies how the Recommendations apply to virtual assets and virtual asset industry participants. However, as noted in comment letters on the draft Guidance, some virtual asset industry participants have described the Guidance as inadequate. For example, industry participants have criticized the Guidance for treating stablecoin central governance bodies that do not, in some circumstances, maintain the authority or provide the services necessary to implement certain AML/CFT requirements as VASPs. Moreover, while the Guidance provides greater clarity on the applicability of the Recommendations on new technologies, important questions remain. For example, the Guidance acknowledges the role of open-source developers of DApp or DeFI applications but does not otherwise provide any specific guidance or advice to regulators on whether and to what extent such developers are subject to AML/CFT requirements.

Nevertheless, the Guidance may have significant implications for entities operating in the virtual asset sector, particularly those that do not currently consider themselves VASPs. For example, the Guidance makes clear that FATF defines the term VASP expansively and expects industry participants that fall within the definition to develop AML/CFT compliance programs. We anticipate that member countries, including the United States, will continue to standardize and update their AML/CFT regulatory regimes in accordance with the FATF Standards. Accordingly, VASPs should consider preemptively assessing their AML/CFT compliance programs against the Guidance in advance of FinCEN rulemaking or other regulatory action FinCEN would need to take to implement the Guidance.

## Background on FATF recommendations for virtual assets and VASPs

While the Recommendations do not have the force of law, FATF members are expected to comply with and implement them. The United States has typically, but not always, adopted the Recommendations or their underlying policies, into national law.[4] In addition to the Recommendations, FATF issues reports and guidance on money laundering risks and typologies. In recent years, FATF has focused its attention on applying the Recommendations to virtual assets and VASPs, particularly through the following:

- **February 2012 Recommendations.** In February 2012, FATF revised its Recommendations to introduce Recommendation 15, "New technologies." Recommendation 15 was intended to address the AML/CFT risks introduced by new products, businesses, and technologies.
- **June 2014 Report.** In June 2014, FATF published a report that outlined potential AML/CFT risks associated with virtual currencies, including (1) limited identification and verification of participants; (2) lack of clarity regarding responsibility for AML/CFT compliance, supervision, and enforcement; and (3) lack of a central oversight body.
- **June 2015 Guidance.** In June 2015, FATF published guidance that outlined risk-based standards for addressing financial crime vulnerabilities associated with virtual currency, focusing primarily on convertible virtual currency and "convertible virtual currency exchangers."
- **October 2018 Amendment to FATF Recommendations.** In October 2018, FATF adopted new definitions of the terms virtual asset and VASP and amended Recommendation 15 to clarify its application to activities or operations involving virtual assets and VASPs.
- **2019 Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (the 2019 Guidance).**[5] In June 2019, FATF published guidance that broadly recommended that countries should require VASPs to comply with the same AML/CFT requirements as traditional financial institutions and provided guidance on the application of Recommendation 16 (the Travel Rule).

In March 2021, FATF announced that it would update the 2019 Guidance, as FATF had committed to do in its 12-month review of the 2019 Guidance and a G20 report on stablecoins. In addition to publishing proposed revisions to the 2019 Guidance, FATF invited public comment from VA industry participants, including specific proposals on the proposed revisions.

# Overview of the guidance

The Guidance underscores the need for countries, VASPs, and other entities involved in virtual asset activities to understand the money laundering and terrorist financing risks associated with such activities and to take appropriate mitigating measures to manage those risks. The Guidance examines how virtual asset activities and VASPs fall within the scope of the FATF Standards. In particular, it discusses the types of activities included in the VASP definition and provides examples of such activities that would fall within that definition as well as those that would potentially be excluded. Further, it highlights the key elements required to qualify as a VASP, which are (1) acting as a business for or on behalf of another person and (2) providing or actively facilitating virtual asset-related activities.

The Guidance also focuses on six key areas: (1) clarifying the definitions of virtual asset and VASP to make clear that these definitions are expansive and there are no situations in which a relevant financial asset is not covered by the FATF Standards (either as a virtual asset or as another financial asset); (2) providing guidance on how the FATF Standards apply to stablecoins and clarifying that a range of entities involved in stablecoin arrangements could qualify as VASPs under the FATF Standards; (3) providing additional guidance on the risks and the tools available to countries to address the money laundering and terrorist financing risks for peer-to-peer transactions; (4) providing updated guidance on the licensing and registration of VASPs; (5) providing additional guidance for the public and private sectors on the implementation of the Travel Rule; and (6) including principles of information-sharing and cooperation among VASP supervisors.

# Application of virtual asset and VASP definitions

The Guidance describes how the definitions of the terms virtual asset and VASP apply to certain virtual asset activities:

- **Stablecoins.** When a central governance or developer body maintains control or influence over the administration and function of a stablecoin, that central body likely qualifies as a VASP, particularly if "the governance body carries out other functions in the stablecoin arrangement." Moreover, if a party manages the development and launch of a stablecoin that does not have an easily identifiable central body, FATF clarifies that "this would create scope for regulatory or supervisory action in the pre-launch phase." The Guidance also provides examples of activities or entities within a stablecoin arrangement that would not be subject to the Guidance, including: "[v]alidators whose

functions are only validating transactions; cloud service providers whose functions are only offering the operation of infrastructure; manufacturers of hardware wallets whose functions are only manufacturing and selling the devices; software providers of unhosted wallets whose functions are only developing and/or selling the software/hardware; merchants which are only providing goods and services in exchange for Coins; software developers who do not undertaken any VASP functions; and individual users."

- **Non-Fungible Tokens (NFTs).** Depending on their specific characteristics, FATF does not generally consider NFTs to be virtual assets, though the determination must be made on a case-by-case basis. FATF notes that industry participants should consider the nature of an NFT, and its functionality in practice, when assessing whether a particular NFT qualifies as a virtual asset. For example, the Guidance states that if an NFT is used for "payment or investment purposes in practice," it would likely qualify as a virtual asset. Conversely, if an NFT is simply a digital representations of other financial assets already covered by the Recommendations, then that NFT would be excluded from the virtual asset definition.
- **Decentralized or Distributed Applications (DApps) and Decentralized Finance (DeFi).** DApps and DeFi applications do not qualify as VASPs because the Recommendations do not apply to underlying technology or software. That said, creators, owners, and operators who control or maintain influence in the arrangement of DApps and DeFi applications may fall under the definition of VASP.[6] Ultimately, owners and operators of DApps and DeFI applications should be distinguished by their control or influence over a DApp or DeFI service's protocol or the assets. However, the Guidance suggests that member countries consider other factors, including "the existence of an ongoing business relationship between [owners/operators] and users" and whether "any party profits from the service or has the ability to set or change parameters to identify the owner/operator of a DeFi arrangement," in determining which entities should be subject to the Recommendations.
- **Unhosted Wallets.** The definition of VASP does not typically cover developers or providers of unhosted wallets, particularly when their only function is to develop and/or sell the software or hardware. However, if an unhosted wallet provider performs virtual asset activities or operations for or on behalf of another person, it would likely qualify as a VASP.[7]

The Guidance acknowledges that virtual asset industry participants and regulators should evaluate the scope and applicability of the Guidance's definitions on a case-by-case basis, paying particular attention to an entity, asset, or technology's role and functionality. However, the Guidance makes clear that almost all of the Recommendations are directly relevant to VASPs, and that VASPs therefore have the same full set of obligations as financial institutions and designated non-financial businesses and professions.

# FATF recommendations applicable to VASPs

## AML program requirements

As established by the Guidance, VASPs and any other entities involved in virtual asset activities should apply each of the compliance measures described in Recommendations 9 to 21 in the same manner as financial institutions. Moreover, the Guidance provides context for how the specific requirements of the Recommendations should be fulfilled and incorporated into a VASP's compliance program.[8] For example, to comply with Recommendation 10, VASPs should, regardless of the nature of the relationship or virtual asset transaction, maintain risk-based customer due diligence (CDD) procedures to effectively verify the identity of new customers, on a risk basis (subject to an occasional transaction *de minimis* threshold of 1,000 USD/EUR). Further, VASPs' CDD procedures should be conducted when VASPs have "suspicions of [money laundering and terrorist financing], regardless of any exemption of thresholds; and where [VASPs] have doubts about the veracity or adequacy of previously obtained identification data." In addition, VASPs should implement enhanced due diligence (EDD) measures for relationships and transactions involving higher-risk countries or customers.[9] Notably, the Guidance provides that VASPs may, under Recommendation 17, rely on adequately regulated third-parties to perform their customer identification and CDD functions.

In addition to CDD/EDD procedures, the Guidance notes that Recommendation 11 requires countries to ensure that VASPs maintain records of "all transactions and CDD measures for at least five years in such a way that individual transactions can be reconstructed and the relevant elements provided swiftly to competent authorities." FATF highlights that public blockchain information may provide a foundation for recordkeeping, as long as VASPs can effectively identify their respective customers, though complete reliance on distributed ledger data is not sufficient.

## Registration and licensing

According to Recommendation 14, countries must register and/or license individuals and entities that provide money or value transfer services (MVTS), and ensure compliance with the country's relevant AML/CFT requirements.[10] The

Guidance also states that Recommendation 14 applies to agents or anyone acting on behalf of MVTS providers. Accordingly, FATF recommends that a VASP should maintain a list of its agents, and consider and include such agents within its AML/CFT compliance programs. Similar to the requirements of Recommendation 14, in the United States, VASPs that qualify as money service businesses (MSBs)[11] are required to register with the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN),[12] and to establish AML/CFT compliance programs in accordance with the Bank Secrecy Act and its implementing regulations.[13]

## Travel rule and suspicious transaction reports

As described above, the 2019 Guidance extended the Travel Rule to VASPs. The Travel Rule includes "the obligations to obtain, hold, and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions with designated persons and entities."[14] FATF recommends that regulators require Originator and Beneficiary entities to make Required Information available to the appropriate authorities, and to freeze or prohibit transactions with designated persons and entities.

FATF also recognizes that not every virtual asset transfer involves two regulated entities—under certain circumstances or arrangements, an Originator or Beneficiary may conduct a transaction with an unhosted wallet or other entity not subject to the Travel Rule. FATF recommends that regulators still ensure that regulated entities continue to collect Required Information, however FATF does not expect that Originators will submit Required Information to individual users who are not regulated entities. Moreover, Beneficiaries receiving a virtual asset transfer from an entity that is not a VASP or regulated entity should still obtain Required Information from their customers. Notably, Required Information does not have to be included directly within the virtual asset transfer on the blockchain; however, FATF recommends that Required Information should be transmitted simultaneously or concurrently with a transaction or transfer of virtual assets. The Guidance notes that VASPs should assess each counterparty VASP's AML/CFT controls to avoid providing Required Information to illicit actors or sanctioned entities, or otherwise to VASPs that cannot adequately protect sensitive information.

The Guidance also recommends that VASPs maintain systems for flagging and reporting suspicious transactions, in accordance with Recommendation 20. In 2020, FATF issued its report on Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing, which provides guidance on identifying and reporting suspicious transactions involving virtual assets. Finally, FATF also recommends that VASPs, like financial institutions, be prohibited from disclosing (i.e., tipping-off) the filing of suspicious transaction reports.

## Economic sanctions

The Guidance states that member countries should require VASPs to screen, and if necessary, block transactions that violate economic sanctions. FATF also notes that VASPs "may need to consider mitigation measures that fit their business process and the technical nature of [virtual assets]." Mitigation measures can include, for example: (a) putting a virtual asset wallet on hold until sanctions screening is completed and the VASP confirms that no violation is committed; and (b) receiving a virtual asset transfer with a provider's virtual asset wallet that links to a customer's virtual asset wallet and moving the transferred virtual asset to a customer's wallet only after sanctions screening is completed.

On October 15, 2021, OFAC published its Sanctions Compliance Guidance for Virtual Currency, stating that "OFAC sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies. Members of the virtual currency industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions … ."

**If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.**


**Kendall Howell**
+1 202 962 7068
kendall.howell@davispolk.com

**Paul Marquardt**
+1 202 962 7156
paul.marquardt@davispolk.com

**John B. Reynolds III**
+1 202 962 7143
john.reynolds@davispolk.com

**Will Schisa**
+1 202 962 7129
will.schisa@davispolk.com

**Daniel P. Stipano**
+1 202 962 7012
dan.stipano@davispolk.com

**Margaret E. Tahyar**
+1 212 450 4379
margaret.tahyar@davispolk.com

**Zachary J. Zweihorn**
+1 202 962 7136
zachary.zweihorn@davispolk.com




1 The United States co-chaired FATF's Virtual Assets Contact Group with Japan. *See* U.S. Treasury Department, *FATF Works to Strengthen Financial Transparency, Combat Misuse of Virtual Assets* (Oct. 21, 2021), https://home.treasury.gov/news/press-releases/jy0423.

2 FATF has also issued nine special recommendations on terrorist financing.

3 FATF is currently comprised of 37 member jurisdictions and two regional organizations, representing most major financial centers across the world. In addition, FATF relies on a global network of FATF-Style Regional Bodies (FSRBs), in addition to its members, to promote the implementation of the Recommendations. Over 200 jurisdictions have committed to the Recommendations through the FSRBs and FATF memberships.

4 FATF's most recent evaluation of the United States in 2016 found that it was fully or largely compliant with 31 of the 40 Recommendations, partially compliant with four of the Recommendations, and non-compliant with five of the Recommendations.

5 In June 2019, the FATF also adopted an Interpretive Note to Recommendation 15, included in the 2019 Guidance as Annex A, to further clarify how the FATF Standards should apply to virtual assets and VASPs.

6 FATF clarifies that this would be the case if other parties have a role in the administration of services for an application or certain activities are otherwise automated. FATF notes that, "[i]t seems quite common for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence."

7 FATF, recognizing the potential risks posed by virtual asset transfers involving unhosted wallets, recommends that VASPs "collect data on their unhosted wallet transfers, and monitor and assess that information as necessary to determine to what extent a transaction is within their risk appetite, and the appropriate risk-based controls to apply to such a transaction/individual customer, and to meet [suspicious transaction reporting] obligations … ."

[8] As noted above, FATF's Recommendations are not legally binding. The applicable regulatory requirements for VASPs operating in the United States remain those established under 31 C.F.R. 1022 and the economic sanctions programs of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC).

[9] FATF observes that, for VASPs, such procedures may involve the use of analysis products such as blockchain analytics.

[10] FATF clarifies that the registration and licensing requirements of Recommendation 15 also apply to all VASPs, even those that engage in MVTS activities.

[11] Under 31 C.F.R. 1010.100(ff), an MSB includes any person who, among other things, does business as a "money transmitter." On March 18, 2013, FinCEN issued guidance that states that "[a]n administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations…"

[12] 31 CFR 1022.380.

[13] 31 CFR 1022.210.

[14] The following information is required under FATF's travel rule (Required Information): (i) the sending customer's (Originator) name; (ii) the Originator's account number when an account is used to process the transaction (e.g., the virtual asset wallet); (iii) the Originator's physical address, national identity number, or customer identification number that uniquely identifies the Originator to the ordering institution, or date and place of birth; (iv) the receiving party's (Beneficiary) name; and (v) the Beneficiary account number when an account is used to process the transaction.