KPMG

# Regulatory Alert

**Regulatory Insights**

**November 2021**

## Virtual assets and related providers | Updated FATF guidance

*As FATF provides additional guidance and continues to broaden what falls under their Recommendations within the virtual asset sector, it gives participating members an understanding on how to incorporate the guidance into their framework, but also highlights the need for careful deliberation for firms that are innovating in the sector, as they await input from their regulators.*

---

FATF has recently released a significant update to its 2019 Guidance for the Virtual Asset (VA) and Virtual Asset Service Provider (VASP) sector. The 2019 Guidance was issued to assist countries and VASPs to understand their anti-money laundering and counter-terrorist financing obligations, and effectively implement the FATF's Recommendations. As a general matter, the Guidance confirms that VASPs are subject to the same relevant FATF measures that apply to financial institutions.

Specifically, the 2021 Update includes additional guidance in the following six key areas:

1. Clarification of the definitions of VAs and VASPs
2. The applicability of FATF Standards to stablecoins
3. The tools available to address money laundering (ML) and terrorist financing (TF) risks for peer-to-peer (P2P) transactions
4. Licensing and registration for VASPs
5. Implementation of the "travel rule" for the public and private sectors
6. Information-sharing and cooperation amongst VASP Supervisors

What follows is a summary of some of the key pronouncements by FATF in the updated Guidelines.

### Definition of Virtual Assets and Virtual Asset Service Providers

The updates to the definitions of VA and VASP were to expand the applicability of the FATF Standards to encompass new types of digital assets and service providers.

— **VAs.** FATF explained that VAs must be digital, digitally traded or transferred, and used for payment or investment purposes. Stablecoins were expressly noted to be subjected to the same FATF standards as a VA or other financial asset. The determinative question for VA designation was described as whether the potential VA has inherent value to be traded or transmitted and is used for payment or investment purposes. Thus, FATF further noted that VAs should not include digital representations of fiat currencies, securities, or other financial assets, nor should they include Central Bank digital currencies (CBDCs). A blockchain-based financial asset may or may not meet the definition, they explained, because the technology used alone is not the deciding factor in determining which FATF Recommendations apply. FATF also spoke to non-fungible tokens (NFTs), noting that digital assets that are "unique, rather than interchangeable, and used as collectibles rather than as payment or investment instruments" are generally not considered VAs

under the FATF definition. Of course, if any asset does not qualify as a VA, it may still be deemed another type of financial asset, such as a security, commodity, derivative, or fiat currency, and thus subject to regulation in any case.

— **VASPs.** FATF's guidance defines a VASP "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 on behalf of another natural or legal person":
  – Exchange between VAs and fiat currencies
  – Exchange between one or more forms of VAs
  – Transfer of VAs
  – Safekeeping or administration of VAs or instruments enabling control over VAs
  – Participation in and provision of financial services related to an issuer's offer and sale of a VA.

  Additionally, the definition of VASPs is not meant to apply to those entities or persons who solely develop underlying code, unless they otherwise provide financial services covered by the VASP definition.

## Stablecoin Guidance

Generally, stablecoins maintain a stable value relative to an underlying reference asset or assets and share many of the same ML/TF risks as other VAs. However, FATF's focus and recent commentary from financial regulators have put a greater spotlight on stablecoins, pointing to what the supervisors say is a significant potential for mass adoption based mainly on the structure and varied uses of stablecoins; their tie to an underlying reference asset and the resulting potential impact on that asset; and their potential use in decentralized platforms. These features also suggest a greater potential for ML/TF, regulatory, or other risks. FATF also provided recommendations to VASPs for steps they could take to attempt to mitigate these risks, such as utilizing blockchain analytic tools to assess relevant wallet addresses, developing an approach to the increased risks posed by unhosted wallets, and engaging with law enforcement and regulatory agencies in the space to enhance the compliance program.

## Tools available to address ML and TF Risks for P2P Transactions

FATF recognizes that P2P transactions may pose greater ML/TF risks, as there are no obliged entities involved, and thus the parties are not adhering to a control environment like that embodied in the Standards. FATF recommends that countries may consider and implement the following to mitigate the risks of P2P transactions:

— Encourage the development of methodologies and tools to assess P2P market metrics and risk mitigation solutions.
— Implement controls that allow for visibility of P2P activity and/or VA activity crossing between obliged entities and non-obliged.
— Develop risk-based supervision of VASPs and entities operating in the VA space.
— Place additional AML/CFT rulesets on VASPs that facilitate transactions with non-obliged entities.
— Apply a risk-based approach to dealing with customers that facilitate P2P transactions.
— Issue public guidance and advisories to raise awareness of risks posed by P2P transactions.

## Travel Rule

In INR. 16, FATF clarifies their Recommendations for the travel rule as it applies to the transfer of VAs. While noting that the information must be transmitted as the transaction takes place ("immediately"), and in a secure manner, INR. 16 does not require that the information be attached to the VA transfer, or that the information be transferred on the blockchain. Rather, the information can be submitted in some other form, such as a batch format, and in fact they note that any solution could be acceptable so long as it complies with the requirements in Recommendation 16 and other AML/CFT obligations.

INR. 16 addresses several other issues around the travel rule, including transaction fees, the sunrise issue, and counterparty VASP due diligence on unhosted wallets. Transaction fees relating to a VA transfer are not within the scope of the travel rule as the party receiving the underlying transfer is not the recipient of the fee. In addition, due to the nature of the product, there are occasions where a VASP must send a greater amount of a VA than the actual amount to be transferred to the beneficiary, with the difference automatically refunded to the ordering VASP. Here too, the added fee would not ordinarily be covered by the travel rule.

On the sunrise issue, FATF explained, "countries are implementing their AML/CFT frameworks for VASPs at different paces…some jurisdictions will require their VASPs to comply with the travel rule prior to other jurisdictions." Countries should adopt a risk-based approach in assessing the business models presented by a VASP and consider the full context of travel rule compliance. As it becomes increasingly difficult to transact with countries that have conflicting AML/CFT

frameworks, FATF provided the following control measures to consider when transacting with VASPs in different jurisdictions:

— Restricting VA transfers to within the VASP's customer base (i.e., internal transfers of VAs within the same VASP)
— Allowing only confirmed first-party transfers outside of their customer base (i.e., the originator and the beneficiary are confirmed to be the same person).

## Enhancing transactions monitoring

The challenges regarding transactions with unhosted wallets are also addressed. FATF states: "In instances in which a VA transfer involves only one obliged entity on either end of the transfer, the obliged entity must adhere to Recommendation 16." At the same time, they note that VASPs are not expected to submit the required information to non-obliged entities. FATF sets forth phased Guidance on how to conduct counterparty due diligence to determine if the counterparty is a VASP and thus establish the requirements for the transaction:

— Phase 1: Determine whether the VA transfer is with a counterparty VASP
— Phase 2: Identify the counterparty VASP
— Phase 3: Assess whether the counterparty VASP is an eligible counterparty who should receive customer data.

## Information Sharing Among VASP Supervisors

In a new section to the Guidance, FATF has developed **Principles of Information-Sharing and Co-operation** between VASP Supervisors across the globe. Throughout the section, FATF presents their vision for a globally cohesive supervisory structure, with respect to the oversight of VASPs and VA activity. The Principles direct the supervisors around the world to:

— Develop an understanding of what information will be useful for authorities, and guidance on the appropriate times to share the information
— Recognize potential triggers for proactive information sharing
— Identify effective methods for sharing information
— Set expectations where multiple supervisors are working together on a specific case or issue
— Suggest potential guidelines when working with VASPs in jurisdictions that do not have sufficient regulatory frameworks in place
— Set out best practice in relation to the types of information countries should maintain on licensed/registered VASPs.

***Relevant links***:
— FATF 2021 Updated Guidance on VAs and VASPs is available here.
— KPMG 2019 Regulatory Alert, Virtual assets and related providers, is available here.
— KPMG 2021 Regulatory Alert, Interagency report on regulation of stablecoins, here.

**For additional information** please contact John Caruso.

# Contact the authors:

**John Caruso**
**Principal**
Forensic Services
johncaruso@kpmg.com

**Amy Matsuo**
**Principal and Leader**
ESG and Regulatory Insights
amatsuo@kpmg.com

**Bianca Nargi**
**Senior Associate**
Forensic Services
bnargi@kpmg.com

**kpmg.com/socialmedia**