CFATF MONTHLY ARTICLE - JULY 2023

Risk-Based Approach to VAs and VASPs: Understanding and Mitigating Risks

Introduction

In this monthly article, the CFATF Secretariat focuses on identifying, assessing and mitigating the ML/TF risks to VAs and VASPs.

Definitions of VAs and VASPs

The FATF Glossary[1] provides the following definitions for VAs and VASPs:

- *Virtual Asset (VA)* - a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations. [2]

- *Virtual Asset Service Provider (VASP)* - any natural or legal person who is not covered elsewhere under the Recommendations and as a business conduct one or more of the following activities or operations for or on behalf of another natural or legal person:

1. Exchange between virtual assets and fiat currencies;

2. Exchange between one or more forms of virtual assets;
3. Transfer of virtual assets; and
4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
5. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Basis for the Risk-Based Approach – VAs and VASPs

Recommendation 1 requires countries to identify, understand, and assess their ML/TF risks and to take action aimed at effectively mitigating those risks[3]. In addition, Recommendation 15, countries are required to assess the risks associated with new technologies and VAs as well as the risks associated with VASPs that engage in or provide covered VA activities, operations, products, or services.

In the 5th Round, countries will be required to ensure that VASPs take steps to identify circumstances in which customers and transactions may present proliferation financing risks, and ensure that their sanctions policies, controls and procedures address these risks, in accordance with national legislation.[4]

Countries should also require VASPs (as well as other obliged entities) to identify, assess, and take effective action to mitigate the ML/TF risks associated with providing or engaging in covered VA activities or associated with offering VA products or services.

VASPs and other obliged entities should assess the ML/TF risks of new products before bringing them to market and put in place mitigation measures before launch.

Supervisors should look for these mitigation measures to be in place before granting registration/licensing and continue on an ongoing basis. It will be more difficult to mitigate risks of these products once they are launched.

Countries have the discretion to ban or limit VA activities, VASPs, and those VA activities carried out by non-obliged entities, based on their assessment of risk and national regulatory context.

In instances where a country decides to ban or limit VAs or VASPs, countries should:

- Identify, understand and assess the associated risks for VAs and VASPs and consider how this action would impact on ML/TF risks.
- Establish additional measures to mitigate the overall ML/TF risks.
- For example, identifying VASPs (or other obliged entities that may engage in VA activities) that may operate illegally in the jurisdiction and applying proportionate and dissuasive sanctions.
- Engage in outreach and enforcement actions based on the country's risk profile.
- Periodically revisit the ML/TF risk assessment of the associated risks and the ability to enforce such a prohibition/limitation may evolve rapidly.

Risk Assessment for VAs and VASPs[5]

The first step in understanding and mitigating risks for VAs and VASPs is to conduct a risk assessment. Relevant risk factors for risk assessment as determined by VASPs and competent authorities can include:

- Types of services
- Products, or transactions involved.
- Customer risk
- Geographical factors

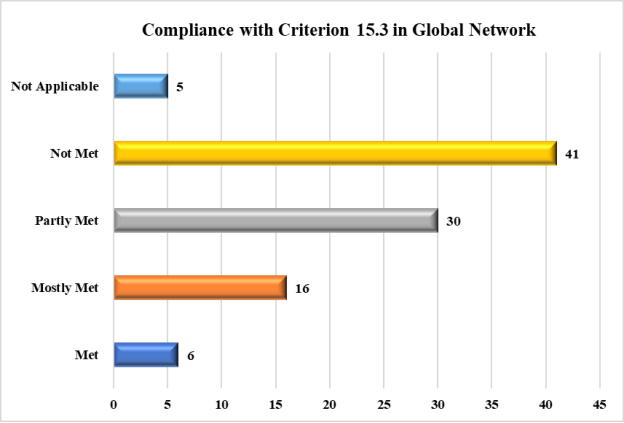
Factors to Consider when Assessing the ML/TF Risks of VAs and VASPs[6]

When assessing VAs or VASPs, respectively, consider whether they are associated with the following risk factors:

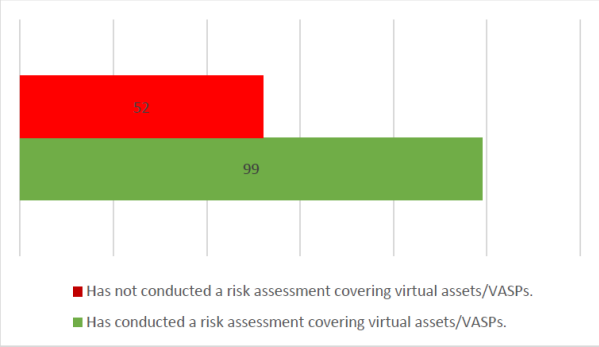
- Facilitates a wide range of financial activities, money or value transfer services to securities, commodities or derivatives-related activity, among others.
- Enables non-face-to-face business relationships.
- Permit transactions to take place without the use or involvement of a VASP or a FI.
- Utilized to quickly move funds globally, in an almost instantaneous and irreversible manner.
- Products or services that facilitate pseudonymous or anonymity-enhanced transactions. Since VAs are cross-border in nature, customer identification and verification measures must be effective to mitigate risks.
- Potentially illicit users can use VAs or VASPs for making payments or transferring funds quickly across the globe or over a wide geographic area.
- VASPs located in one jurisdiction may offer their products and services to customers located in another jurisdiction where they may be subject to different AML/CFT obligations and oversight. Risks can increase when there are weak/non-existent AML/CFT controls or limited international co-operation.
- Large number and types of providers in the VA space and their presence across multiple jurisdictions. Risks can increase when there is a lack of clarity on which entities or persons (natural or legal) involved in the transaction are subject to AML/CFT measures and which countries are responsible for regulation.
- Peer to peer (P2P)[7] can potentially be used to avoid AML/CFT controls in the FATF Standards since there is no involvement of VASP or other obliged entity and not subject to AML/CFT controls.

Global Network Compliance with conducting VA and VASP Risk Assessments

Criterion 15.3 of the FATF Methodology focuses on risk assessment and application of a risk-based approach. As of April 2023, out of the 98 countries assessed, for criterion 15.3 the chart shows the ratings achieved.[8] Based on mutual evaluation and follow-up results, 71 of 98 jurisdictions (72%) are not sufficiently implementing this requirement, being rated as “partially met or not met”.



In a survey of 151 jurisdictions, when asked if the country has conducted a risk assessment of VAs/ VASPs, the FATF reported the following.[9]



Challenges to assessing ML/TF risks of VAs and VASPs[10]

The FATF states that countries reported two common challenges undertaking a risk assessment:

1. A lack of reliable and easily available data, for example on VA usage, the VASP population, the extent of suspicious or illicit transactions.
2. Limited guidance or methodologies on conducting such a risk assessment.

The FATF encourages countries to refer to the FATF 2021 *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* which includes factors that jurisdictions should consider when conducting a VA/VASP risk assessment.

Recommendations for the public and private sectors – VA/VASP risk assessments and mitigation[11]

- Countries that have not conducted risk assessments of VAs and VASPs should utilize available resources, including the FATF's 2021 guidance to identify the risks, and put implement the necessary risk mitigation measures.
- Jurisdictions that permit VAs and VASPs and those that prohibit them should establish or continue monitoring/supervision measures against non-compliance, including sanctioning illicit VASPs.
- Jurisdictions should take immediate action to mitigate increasing TF and PF threats related to VAs, including the full implementation of R.15 and adopting other risk-based measures, such as enhancing cybersecurity.
- Countries are encouraged to assess and monitor the risks associated with unhosted wallets, including P2P transactions, share experiences and best practices on, inter alia, data collection, risk assessment methodologies, findings and mitigating risks.
- The private sector, particularly VASPs, should have appropriate risk identification and mitigation measures in line with R.15 due to increasing TF and PF threats related to VAs. Other risk-based measures, such as cyber security measures should be adopted.
- The private sector should continue to monitor and assess the risks across the VA ecosystem, take steps to mitigate these risks and to consult with regulators as necessary to ensure a common risk understanding.

References

[1] FATF (2012-2023)," International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation", FATF, Paris, France, p. 135.

[2] Please keep in mind that para. 1 of INR 15 states that "for the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)".

[3] FATF. 2021. "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" FATF, Paris, p. 38 - 39

[4] See PF requirements in FATF. 2021, p. 37 "Guidance on Proliferation Financing Risk Assessment and Mitigation."

[5] FATF. 2023. "Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs", FATF, Paris, France, p. 16

[6] FATF. 2021. "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" FATF, Paris, p. 16

[7] The FATF defines peer-to-peer (P2P) transactions as VA transfers 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).

[8] FATF. 2023. “Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs”, FATF, Paris, France, p. 11

[9] Ibid, p. 12

[10] Ibid

[11] FATF. 2023. “Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs”, FATF, Paris, France, p. 35