Summary of the risk assessment of money laundering and terrorist financing for virtual asset service providers

26.11.2024

Contents

In brief

The Financial Supervisory Authority (FIN-FSA) has prepared a sectoral risk assessment of money laundering and terrorist financing for the virtual asset service providers it supervises.

According to the risk assessment, the risk related to both money laundering and terrorist financing facing the sector as a whole is significant, i.e. the second highest on a four-step scale.

Real-time activity and global mobility increase the risk associated with virtual assets, both in terms of money laundering and terrorist financing. Consequently, the provision of virtual asset services also carries the risk of criminally acquired funds being transferred globally and quickly via the services.

In addition, information regularly collected by the FIN-FSA and supervisory measures have revealed deficiencies in the risk controls of virtual asset service providers.

1 Purpose and scope of the sectoral risk assessment

The sectoral risk assessment is the FIN-FSA's assessment of the money laundering and terrorist financing risks for virtual asset service providers at a sectoral level. In the FIN-FSA's inherent risk assessment on money laundering and terrorist financing, the risks related to different sectors were examined at the top level and only from the standpoint of the products and services typically provided in the sectors. For the sectoral risk assessment, a more in-depth analysis has been conducted of the products and services, customers, distribution channels and geographical coverage of virtual asset service providers registered under the Act on Virtual Asset Service Providers (572/2019). In addition, risk controls have also been taken into account. The assessment is formed at the sector level, however, not at the level of individual supervised entities.

The risk assessment will guide the FIN-FSA in targeting supervisory resources and selecting supervisory measures on the basis of risk. In accordance with the guidelines on risk-based supervision issued by the European Banking Authority (EBA), the FIN-FSA must prepare a supervision strategy for preventing money laundering and terrorist financing, a key element of which are risk assessments for the various supervised sectors.

Regulations regarding virtual asset service providers have changed significantly during 2024. Regulation (EU) 2023/1114 on markets in crypto-assets (hereinafter the MiCA Regulation) was adopted on 31 May 2024. Due to the MiCA Regulation, a new Act on Crypto-Asset Service Providers and Crypto-Asset Markets (402/2024) was enacted, which entered into force on 30 June 2024 and repealed the Act of Virtual Asset Service Providers. Entities entered in the register of virtual asset service providers must apply for authorisation in accordance with the MiCA Regulation if they intend to continue providing services.

This risk assessment reflects the situation of the sector at a time of regulatory change, i.e. in August 2024, when 13 virtual asset service providers were entered in the FIN-FSA's register and no authorisation applications under the new regulations had yet been received. Of those entered in the register, six were already registered following the entry into force of national legislation in 2019 and the rest thereafter.

As already evident from the names of the regulations, following the European regulations the term *crypto asset* will be used in the future instead of virtual asset, and the term *crypto asset service provider* (CASP) will be used instead of *virtual asset service provider* (*VASP*).

As this risk assessment still concerns registrations granted under the old regulations, the terms used are those according to the old regulations, i.e. virtual asset service provider (VASP) and virtual asset.

2 Preparation of the risk assessment

When assessing the risks of money laundering and terrorist financing, the FIN-FSA uses a four-step scale, which corresponds to the scale used by the EBA[1]. For each risk level, a corresponding risk score has been determined to describe it.

Risk level	Risk score corresponding to the risk level
Very significant	4
Significant	3
Moderately significant	2
Less significant	1

The sectoral risk assessment is prepared by assessing the risk level associated with the following risk categories and risk control categories:

- Risk categories:
  - Products and services
  - Geographical location
  - Customers
  - Distribution channels
- Control categories:
  - Risk-based approach
  - Organisation of activities
  - Customer due diligence
  - Monitoring

Both the risk and control categories are assessed according to how much risk is associated with them. Also, with regard to controls, attention is focused on the deficiencies of the controls and the risk-increasing effect of these deficiencies.

The overall risk level is the aggregate assessment formed from the risk levels of the risk categories and the control categories. The risk level of the risk categories has been weighted more relative to the control categories. The reason for this is that it is not possible, and it is not always appropriate to try to completely eliminate the risk of money laundering or terrorist financing through controls. In addition, the perception of controls is largely based on the data reported by supervised entities through the RA data collection[2], which have not been verified by supervisory measures.

When preparing the risk assessment, the following information, among other things, was used

- Information supplied to the FIN-FSA in connection with VASP registrations, data reported through the RA data collection (on 31 December 2023) and information obtained in connection with supervisory measures.
- Annual reports of the Financial Intelligence Unit of the National Bureau of Investigation and data obtained through cooperation with authorities.

[1] EBA The Risk-Based Supervision Guidelines EBA/GL/2021/16, chapter 4.3.6

[2] FIN-FSA's annual data collection on risks and controls related to money laundering and terrorist financing and sanctions (RA, Risk assessment survey)

- The FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021) and meetings of the Virtual Asset Contact Group
- European Banking Authority
    - Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector. Paris, France 2023
    - Guidelines EBA/GL/2021/02 on ML/TF risk factors including amendments EBA/GL/2024/01
- REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM (2022) 554 final) and (COM (2019) 370 final)
- National risk assessment of money laundering and terrorist financing 2021 (publications of the Ministry of Finance 2021:12) and Risk assessment 2023: partial update (Publications of the Ministry of Finance 2024:8)

3 Risk assessment and its justifications

3.1 Results of the sectoral risk assessment

In the FIN-FSA's assessment, the overall risk related to money laundering and terrorist financing in the virtual assets service provider sector is **significant**.

The overall risk is the same from the perspective of both money laundering and terrorist financing. This is based on the fact that, in practice, the same elements in products and services increase the risk of both money laundering and terrorist financing. With regard to geographical risk and risks associated with customers and distribution channels, money laundering and terrorist financing have not yet been separated at the level of sectoral risk assessment. The reason for this is that, at the sector level, it is not possible to review, for example, payment traffic on a country-by-country basis in order to determine whether payment traffic is directed to areas associated with an increased risk of terrorist financing. A more detailed analysis may made as part of supervised-entity-specific risk assessments, which may be taken into account later when updating the sectoral risk assessment. With regard to controls, the controls for money laundering and terrorist financing have also been assessed as a single entity.

In the risk assessment, the risk associated with products and services has been weighted relative to other risk factors. The justification for this is that products and services determine how a sector, subsector or individual entity may be exploited for money laundering or terrorist financing. Without products or services that involve a risk of money laundering or terrorist financing, it is difficult for the sector to be exploited for money laundering or terrorist financing.

The risk scores corresponding to the risk levels determined for the risk and control categories are shown in the table below:

Risk categories:	
Products and services	4
Geographical location	2
Customers	3
Distribution channels	3
Risk level of risk categories:	**3**
Control categories	
Risk-based approach	3
Organisation of operations	3
Customer due diligence	4
Monitoring	3
Risk level of control categories:	**3**
Overall risk level of the sector	**3**

3.2 Risk categories

3.2.1 Products and services

The products and services provided play a decisive role in the risk of a sector or individual entity being exploited in money laundering.

A starting point for the assessment of risks associated with products and services is the FIN-FSA's inherent risk assessment on money laundering and terrorist financing and the inherent risk levels determined therein for different products and services. In the inherent risk assessment published by the FIN-FSA in 2022, the inherent risk level of both money laundering and terrorist financing related to virtual asset services is assessed as being significant.

It is possible to transfer virtual assets nearly or completely in real time and to anywhere in the world. The effects of real-time activity are particularly enhanced by widely used automatic trading bots. In addition, approved transactions are irrevocable. This almost exclusively concerns online transactions that are executed without the parties meeting face-to-face. Virtual currencies can be transferred and deposited using virtual asset service providers, but individuals can also transfer funds to each other without the involvement of a service provider. The virtual asset therefore acts like electronic cash that can be circulated globally without restrictions. However, a service provider is, in practice, always needed to exchange a virtual asset into fiat currency and vice versa. In the global market, there are a number of service providers specialised in this kind of activity that do not adhere to, for example, the rules regarding customer due diligence. Moreover, the Financial Intelligence Unit, in its own analysis, has also found that rapid transfers and international operations are characteristic of the virtual asset service sector.[3]

Real-time activity and global mobility increase the risk associated with virtual assets, both in terms of money laundering and terrorist financing. Another challenge is raised by the fact that the sector has only been regulated for a short period of time and, particularly in areas other than prevention of money laundering and terrorist financing, such regulation has been rather light. The sector provides services globally across borders and it is not always easy to determine supervisory responsibilities and organise supervision.

The methods of money laundering and terrorist financing with regard to virtual asset services largely correspond to the methods identified in the banking and payment services sector: the goal is to conceal the criminal origin of funds by transferring a virtual asset from one wallet and service to another and by depositing and withdrawing funds as fiat currency. As stated above, the fact that funds can also be transferred from outside the supervised service providers raises its own challenge.

Collecting funds for terrorist organisations in virtual assets has been identified as a phenomenon of financing terrorism. Funds have been collected simply by posting on social media wallet addresses to which funds can be sent.

Under section 2, subsection 1, paragraph 6 of the Act on Virtual Asset Service Providers, virtual asset services include the issuance of virtual assets, virtual asset exchange services and wallet services. Registered VASPs provide either an exchange service and/or a wallet service. On a service-specific basis, the risk of both money laundering and terrorist financing is significant for exchange services. The risk of money laundering is also significant for wallet services. The risk of terrorist financing can be considered to be slightly lower for wallet services to which funds can only be transferred by the owner of the wallet, i.e. an identified and verified customer of the service provider.

[3] Financial Intelligence Unit, Annual Report 2022, p. 17 (in Finnish).

Taking into account the products and services of VASPs operating in the sector and the risk-increasing factors referred to in the EBA Guidelines on risk factors related to these products and services (EBA/GL/2024/01), the overall risk of the products and services is **very significant**.

3.2.2 Geographical location risk

The risk related to geographical location is assessed as being **moderately significant**.

National regulations have not granted domestic VASPs the opportunity to provide services to other EU or non-EU countries on the basis of their registration. In order to provide virtual asset services outside Finland, VASPs registered in Finland have had to apply for authorisation or register as required by the target country's regulations. Some of the VASPs entered in the register have links to the EU due to their group structure, thereby increasing the geographical risk compared with purely national activities. Some VASPs are also permitted under some other authorisation to provide part of their services on a cross-border basis within the EEA.

3.2.3 Customer risk

The risk related to customers has been assessed as being **significant**.

In assessing the risk related to customers, the data reported in the RA data collection about different client groups have been taken into account. Both absolute and percentage customer numbers have been taken into account, for example with regard to high-risk customers and customers located abroad. Failure of supervised entities to identify high-risk customers also affects the risk.

3.2.4 Distribution channel risk

The risk related to distribution channels has been assessed as being **significant**.

The risk is impacted by, among other things, the fact that services are provided in the sector via remote services without verifying the customer's identity using the verification referred to in chapter 3, section 11, subsection 1, paragraph 3 of the Money Laundering Act. When offering services, VASPs use foreign partners of whose risk controls the VASP does not necessarily have a comprehensive understanding.

3.3 Control categories

3.3.1 Risk-based approach

Through the RA data collection, VASPs have reported that they have taken into account all regulatory requirements in their risk assessment and that they classify customers into risk categories. The supervision has revealed, however, that for some supervised entities risk assessment remains superficial and the risk classification of customers is based only on individual risk factors. In addition, the risk category assigned to a customer may not always correspond to the risks identified in the company's risk assessment. The risk assessment should comprehensively review the risks of money laundering and terrorist financing related to the supervised entity's operations, and the identified risks should be considered when determining the customer's risk category and ongoing supervisory measures.

3.3.2 Organisation of operations

Through the RA data collection, VASPs have reported that, during the last two years, they have drawn up or updated operating principles, codes of conduct and work instructions regarding the prevention of money laundering and

terrorist financing. Supervision has found, however, that instructions do not always specify in sufficient detail and in a practical way the measures required to comply with customer due diligence obligations. This leads to the fact that customer due diligence obligations are not necessarily consistently applied. The organisation of tasks in supervised entities has also proved to be inadequate. Responsibilities related to control and monitoring of compliance with obligations are not always clearly defined.

3.3.3 Customer due diligence

Regarding customer due diligence controls, it can be stated that VASPs have various remote identification solutions available when establishing a customer relationship. These solutions are not the means of identification referred to in chapter 3, section 11, subsection 1, paragraph 3 of the Money Laundering Act. In connection with so-called innovative identification solutions, the guidelines issued by the EBA on the subject should be followed. Supervision has found that VASPs are not always sufficiently familiar with how the remote identification solutions they use work. VASPs have also reported that they outsource customer due diligence measures and use third parties without a detailed description of processes and responsibilities. Deficiencies have been identified in updating customer due diligence information and in enhanced identification procedures.

3.3.4 Monitoring

Due to the nature of virtual asset transactions, the FIN-FSA has recommended that VASPs have an information system-based monitoring system in place so that they can effectively monitor customer transactions. Blockchain analysis software of various kinds is an essential element in monitoring the movement of funds and identifying the origin of funds and where they might be going. Almost all VASPs reporting through the RA data collection use an external service provider’s analysis software for transaction monitoring, and some have also developed their own analysis software. It is alarming, however, that in ongoing monitoring, some VASPs use only a few scenarios as a basis for monitoring customers’ activities and payment traffic. VASPs also vary in how quickly they react to alerts generated by monitoring. Most VASPs make very few suspicious transaction reports to the Financial Intelligence Unit.

4 Targeting of supervision

In its 2022 inherent risk assessment, the FIN-FSA published its assessment of the significance of each of its supervised sectors in combating money laundering and terrorist financing, using the same four-step scale used in sectoral risk assessments. In terms of risk, virtual asset service providers were classified as a significant (3) sector, considering the inherent risk of the sector and the number of customers. During 2024, two inspections were targeted at the sector.

With the entry into force of the MiCA Regulation, VASPs entered in the FIN-FSA's register must apply for authorisation as a crypto-asset service provider if they intend to continue offering services. A prerequisite for authorisation as a crypto-asset service provider is compliance with the obligations set by regulations on preventing money laundering and terrorist financing. The authorisation process will therefore include a detailed review of the operating principles, codes of conduct and internal controls of all applicants seeking authorisation, with particular attention to any deficiencies identified in preparing a risk assessment.