



Feedback by the Financial Intelligence Unit to virtual asset service providers about the year 2021

Risk environment

In Estonia, 81–118 million euros (up to about 120 million euros) of criminal proceeds are generated annually through national crime, which could be laundered¹. Primarily, this amount breaks down between the following predicate offences: drug offences (30–50 million euros), fraud (37–40 million euros), embezzlement (10–20 million euros) and tax offences (4–8 million). The turnover of the cross-border payments by the banks operating in Estonia (86.2 billion euros in 2021) and the volume of the transactions mediated through virtual asset service providers (20.3 billion euros between July 2020 and July 2021) are several times higher, indicating a **higher risk of cross-border money laundering**. This is also confirmed by the information on the foreign inquiries sent to the Financial Intelligence Unit (hereinafter: FIU): the amount related to foreign inquiries sent to the FIU in 2021² was 1.33 billion euros, half of which passed through Estonia in transit.

The foreign inquiries sent to the FIU also show that Estonia hosts the **layering** phase of the assets received from abroad, and that fraud (65%) and tax fraud (10%) committed abroad dominate in the foreign inquiries and spontaneous information disclosures as suspected predicate offences. The most common type of money laundering in the foreign inquiries sent in 2021 was the **transfer of funds obtained by fraud to the IBAN account of a foreign payment service provider or virtual asset service provider** and the subsequent transfer thereof through the respective service provider's platform. This trend has grown over time.

According to the Estonian National Money Laundering and Terrorist Financing Risk Assessment (NRA 2020), completed in 2021³, virtual asset service providers are the **riskiest sector in terms of money laundering and terrorist financing**. The same conclusion was drawn by the FIU in its risk assessment completed at the beginning of 2022⁴, where the main conclusion was that the implementation of the due diligence measures by service providers with an Estonian authorisation is remarkably inadequate and which, when comparing the volume of service provision, the low level of skills and knowledge of the staff responsible for

¹ Source: Sectoral risk assessment by the Ministry of Finance in 2021

² 2021 Financial Intelligence Unit Annual Overview of International Cooperation
[<https://fiu.ee/media/246/download>]

³ Vulnerability of the financial technology sector. National Risk Assessment. Ministry of Finance, 2021.
[<https://www.fin.ee/media/1777/download>].

Analysis of the risks of virtual asset service providers 2020–2021. National Risk Assessment. Ministry of Finance, 2021. [<https://www.fin.ee/media/1791/download>]

⁴ The risks related to virtual asset service providers in Estonia. Financial Intelligence Unit, 2022,
<https://fiu.ee/media/170/download>.

preventing money laundering and terrorist financing and financial sanctions, continues to indicate high risks in the sector.

In Estonia, like elsewhere in the world, criminal offenders increasingly use virtual currencies to “launder” the proceeds of crime. In terms of **money laundering**, the NRA 2020 identified the main risks for virtual asset service providers to be the lack of transparency in the sector, the absence of a full risk map of the sector, insufficient requirements for the applicants for authorisations, poor supervision capacity and short inspection time, higher risk due to e-residents, difficulty in on-site supervision, no actual link of the market participants with Estonia, rapid growth in the number of service providers, and the highly differing quality of the due diligence measures applied by market participants. According to the NRA 2020, the greatest risks in terms of **terrorist financing** were high anonymity, lack of transparency in the sector, difficulty in on-site supervision and no actual link of the service providers with Estonia.

Of the 673 foreign inquiries and spontaneous information disclosures sent to the FIU in 2021, 107 concerned virtual asset service providers. These inquiries relate to a time a few years ago where the turnover of virtual asset service providers was eight times lower than today. Knowing this, we predict that the number of foreign inquiries will increase even further in the future.

According to Europol, the use of virtual currencies is in an upward trend due to criminal activities and money laundering, but the share of transactions in virtual currencies in shadow economy is still modest compared to the use of cash and other types of transactions⁵. According to Chainalysis, cybercriminals might have laundered 8.6 billion US dollars worth of virtual currencies in 2021. Compared to 2020, this is a 30% growth, taking into account cybercrime where assets were not exchanged from regular currency to virtual currency.⁶

However, the use of virtual currencies is no longer related to cybercrime only, but is increasingly more being used for different types of crime where transactions of property value need to be made, such as drug trafficking, hiring a contract killer on the dark web, various types of fraud, human trafficking, etc⁷.

Overview of the reports sent in 2021

In 2019, virtual asset service providers filed 400 reports to the FIU and 530 in 2020, but **1,865** in 2021, which made up 11% of all reports. The reporting activity of virtual asset service providers is showing signs of improvement, but the receipt of only a few reports from service providers with the highest turnover is a sign of risk. In 2021, **101 virtual asset service providers** filed reports.

⁵ <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>

⁶ <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/>

⁷ Analysis of the risks of virtual asset service providers 2020–2021. National Risk Assessment. Ministry of Finance, 2021. [<https://www.fin.ee/media/1791/download>]

Table 1. Breakdown of the reports sent to the FIU by groups of reporting entities in 2021

Reporting group	Total	Total (%)	ML	ML (%)	TFR	TFR (%)	ISR	ISR (%)
Credit institutions	11,074	66.5%	10,988	78.1%	2	0.7%	81	81.8%
Financial institutions	2,088	12.5%	813	5.8%	223	73.6%	3	3.0%
Virtual asset service providers	1,865	11.2%	1,781	12.7%	67	22.1%	4	4.0%
Agencies and persons from other countries	709	4.3%	32	0.2%	0	0.0%	2	2.0%
Professionals	282	1.7%	151	1.1%	8	2.6%	1	1.0%
Public agencies	199	1.2%	32	0.2%	1	0.3%	3	3.0%
Non-obliged subject	185	1.1%	180	1.3%	0	0.0%	0	0.0%
Gambling operators	143	0.9%	57	0.4%	0	0.0%	0	0.0%
Other private entities	110	0.7%	29	0.2%	2	0.7%	5	5.1%
TOTAL	16,655	100%	14,063	100%	303	100%	99	100%

Details: “ML” – report concerning money laundering (STR, UTRs and UARs), “TFR” – Terrorist Financing Report (TFR and TR_UAR); “ISR” – International Sanctions Report.

Virtual asset service providers play a very important role across the reporting groups, especially as they are a high-risk sector, and the reports they file allow the FIU to assess the trends and risks in the market.

The largest share of the reports filed by virtual asset service providers were related to money laundering – 1,273 Suspicious Transaction Reports (**STR**), 255 Unusual Transaction Reports (**UTR**) and 253 Unusual Activity Reports (**UAR**) were filed. In total, 67 terrorism-related reports were filed, the majority of them, 63, were Unusual Activity Reports related to a high-risk country (**TR_UAR**) and 4 were Terrorist Financing Reports (**TFR**). A total of 4 reports concerning suspicion of violation of sanctions (**ISR**) were filed. In 2021, virtual asset service providers filed 13 Currency Transaction Reports (**CTR**).

In the case of reports from virtual asset service providers, the main keywords to be pointed out are counterfeit document, unclear origin of assets, identity theft, and the dark web. In the analysis by the FIU, the reports from virtual asset service providers play a very important role. Of the reports filed to the FIU in 2021, **8** were sent for in-depth analysis. The low number of reports sent for in-depth analysis is due to the fact that the cases reported were often unrelated to Estonia. In addition to the case studies, the FIU also used the information received from the reports in its strategic analyses – in risk assessments and thematic surveys.

In 2021, according to the reports by virtual asset service providers, a restriction was imposed on an account or on the use of assets on an account on **one** occasion. In the materials sent to Estonian investigative bodies, the data contained in **69** reports were used.

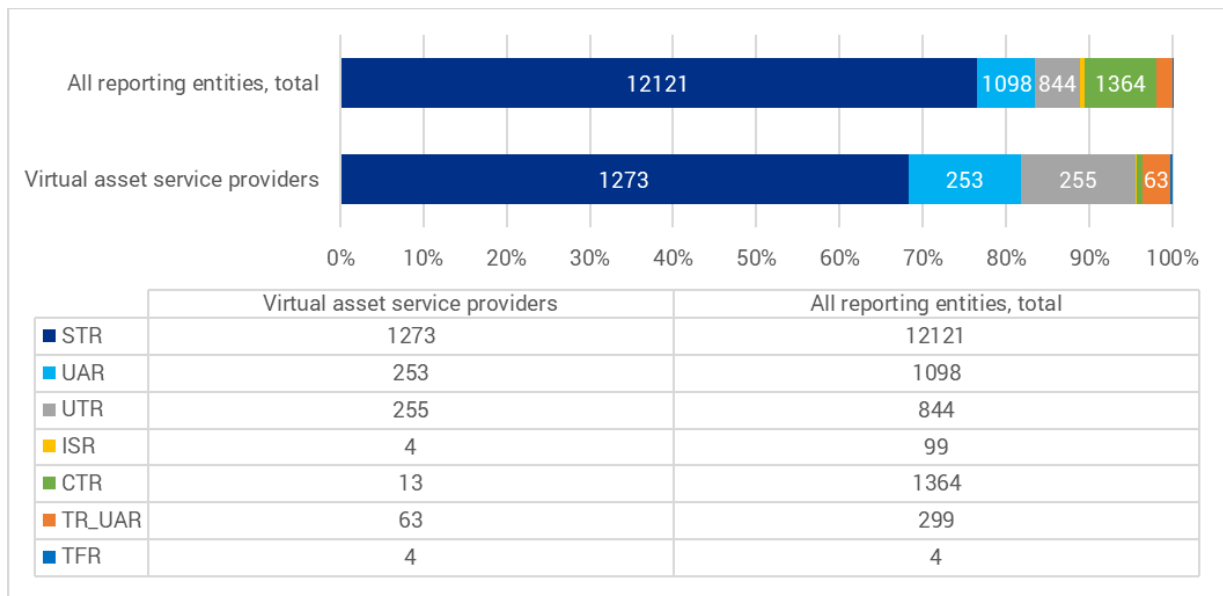


Figure 1. Breakdown of the reports sent by virtual asset service providers and all reporting entities to the FIU in 2021 by report types.

Similarly to 2020, the most frequent reason noted for filing a report was that there are doubts as to the truthfulness of the data submitted by the person (1.2. STR). The other most common reasons were unusual transactions or unusual transactions with virtual currencies (2.3 and 4. UTR), or that a person with a reporting obligation refuses to enter into a customer relationship due to being unable to perform due diligence measures (1.3. STR).

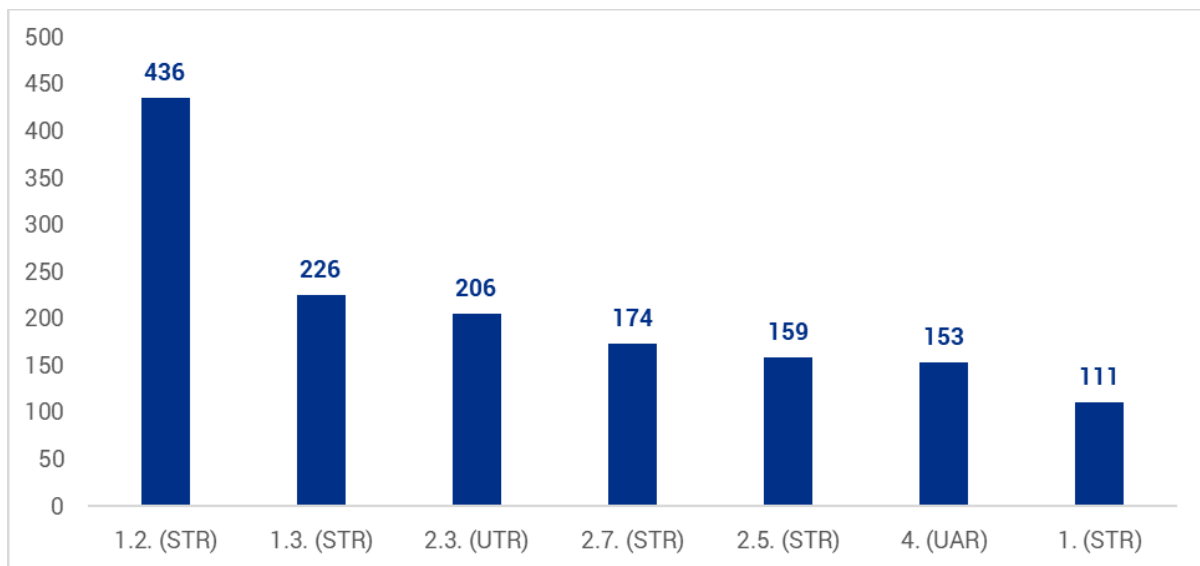


Figure 2. The most common indicators in the reports sent by virtual asset service providers to the FIU in 2021.

- 1.2. (STR)** Doubts as to the truthfulness of the data submitted by the person
- 1.3. (STR)** A credit or financial institution refuses to enter into a business relationship with a person or terminates a business relationship in accordance with the provisions of § 42 of the MLTFPA due to the impossibility of performing due diligence measures
- 2.3. (UTR)** Unusual transaction in virtual currency
- 2.7. (STR)** A suspicion that the property being the object of the transaction is an object of fraud or it is used for money laundering (transactions of a misled person)

- 2.5. (STR) A person fails to provide explanations or documents about the transaction to the extent necessary to perform due diligence measures or the information submitted is not plausible (MLTFPA § 42 (1) occasional transaction and § 43 (1) transaction of a person in customer relationship)
- 4. (UAR) Unusual transactions in virtual currency
- 1. (STR) At the time of establishing a business relationship / entering into a contract with a customer

Quality of the reports, and recommendations for the future

Over time, the reports have become more informative and the circle of reporting entities has expanded, but the FIU's content analysis of the reports revealed that many market participants had shortcomings in the identification of suspicious transactions. The quality of the reports submitted by virtual asset service providers is good. There are few formal and substantive errors, of which only a few are worthy of mention: incorrect type of report or indicator and the often unjustified note "urgent" on the report, especially where the customer relationship has been abandoned or the transaction has already been executed. However, a report that explains the plan for abandoning a customer relationship should clearly indicate the time frame for terminating the relationship.

While the sector's reporting activity has improved, it still remains insufficient, which also indicates a generally low level of the performance of due diligence measures. Transactions (including the origin of the assets from mixed sources) are not sufficiently analysed, not to mention reflecting such information in the reports. Nearly a tenth of the reports were incomplete or had errors in form. Of the 52 reports marked "urgent", 18 were incomplete or had the reason or report type stated incorrectly.

The biggest shortcoming of the reports from the virtual asset service provider sector is that the reporting entity does not understand the content of the business relationship. The description of the transaction is often brief and does not state the reasons for the report. The report is filed without first assessing or analysing it. Instead, report documents are supplemented with additional documents that are often irrelevant and do not support the content of the report. According to the FIU, cases like this are the so-called defensive reporting (a report is filed prematurely with a superficial explanation of the reasons for the report and without confirming the doubts; the FIU started analysing defensive reporting more thoroughly in the second half of 2021), showing that the report is only filed in fear of being punished for not filing it. In addition, the FIU has noted that a virtual asset service provider often lacks the ability and means to analyse transactions, and that there are no monitoring systems in place to suspend suspicious transactions on time. Interaction with the sector shows that the transmission of a response to an inquiry made within a report to the FIU is delayed, not sent at all, or the response is confusing and irrelevant.

Given the size, volume and **high risk level** of the sector, virtual asset service providers filed reports concerning terrorist financing in **disproportionately low** numbers, and **only four** service providers filed them.

On 25 April 2022, the FIU updated the **guidelines on the characteristics of suspicious transactions**⁸, as well as the system for filing reports referring to terrorist financing. As regards TFRs, the virtual asset service provider sector has a three-month transition period to bring its monitoring and reporting systems into compliance with the guidelines. Thus, technical readiness must be ensured by 25 July 2022 at the latest, but reports can be filed earlier already, according to the new guidelines. Two types of Terrorist Financing Reports are distinguished: TFR-1 and TFR-2. **In addition to the connection of the transaction party to a high-risk country, TFR-1 presumes the existence of a fact referring to a specific suspicion of terrorist financing, that is, a suspicion indicator.** The risk and suspicion indicators to be included in the report are available in the guidelines. On its website, the **FIU published**, as an annex to the guidelines, the list of countries at a higher risk of terrorist financing, i.e., the **list of high-risk countries**.

The improved guidelines on the characteristics of suspicious transactions also include additional indicators for international sanctions. This contributes to the quality of the ISRs, as an indicator has been added which requires reporting of other sanctions not mandatorily imposed by Estonian regulations, such as the US and UK sanctions.

It is important to note that in 2022, the EU imposed restrictions on cryptoassets for the first time. For example, in the EU Council Regulation 833/2014, “transferable securities” are now also in the form of cryptoassets traded in capital markets, except for payment instruments. Article 5 (b) 2) of the same EU Regulation prohibits, inter alia, the provision of cryptoasset wallet, account or custody services to Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia, if the total value of cryptoassets of the natural or legal person, entity or body per wallet, account or custody provider exceeds EUR 10,000. With regard to the restriction on such services, the FIU expects VASPs to file reports under the ISR indicator 3, in particular.

Observations from the supervision by the Financial Intelligence Unit


In 2021, we revoked the authorisations of 329 VASPs and launched 18 supervisory procedures concerning VASPs. Given the results of the NRA 2020 and the so-called first survey of virtual asset service providers⁹ (completed in 2020), the FIU also paid a lot of attention to the sector in the 2021 supervision activities – this sector underwent the most supervision inspections.

In the supervision inspections, the FIU identified shortcomings in all of the inspected companies. The main shortcomings were found in procedural rules, risk assessment and performance of due diligence measures. This is consistent with the results of the survey by the FIU, and the NRA.

As of 31 December 2021, 381 virtual asset service providers had a valid authorisation in Estonia. The due diligence measures of the vast majority of virtual asset service providers

⁸ Guidelines on the characteristics of suspicious transactions. Financial Intelligence Unit, 25 April 2022, <https://fiu.ee/media/264/download>.

⁹ Survey of virtual asset service providers. Financial Intelligence Unit, 2020, <https://fiu.ee/media/68/download>.



are not in compliance with the risks, the customer base size or the volume of services provided, neither upon the establishment of, nor during, customer relationships. In the supervision inspections, the FIU has identified a number of shortcomings in the rules of procedure as well as in the risk assessments: failure to correctly apply due diligence measures or identify politically exposed persons or beneficial owners, etc.

In the summer of 2021, the FIU conducted a survey among VASPs. We asked for information on turnovers, wallets and customers. We revoked the authorisations of those who did not respond to the precept (questionnaire) and had not started providing the service within 6 months after being granted the authorisation.