Feedback by the FIU to virtual currency service providers

Overview of the reports sent by Estonian virtual currency service providers to the FIU in 2020, and their use by the FIU

In 2020, virtual currency service providers sent 530 reports to the FIU, which accounted for 6.4% of all reports. The reporting obligation has improved to a certain extent in the virtual currency sector, both in terms of the total number of reports submitted (405 submitted in 2019) and, more importantly, in terms of the number of reporting entities. In 2020, reports were submitted by 45 virtual currency service providers, whereas a year earlier, when almost three times as many companies were authorised, only 16 service providers sent reports. Also, most of the reports were no longer received from just two reporting entities; the number of reports submitted was considerably more consistent across companies. Nevertheless, the number of reporting entities is low, considering the total number of service providers; there are close to 450 market participants[1]. 28 reports (about 5%) were marked "urgent".

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

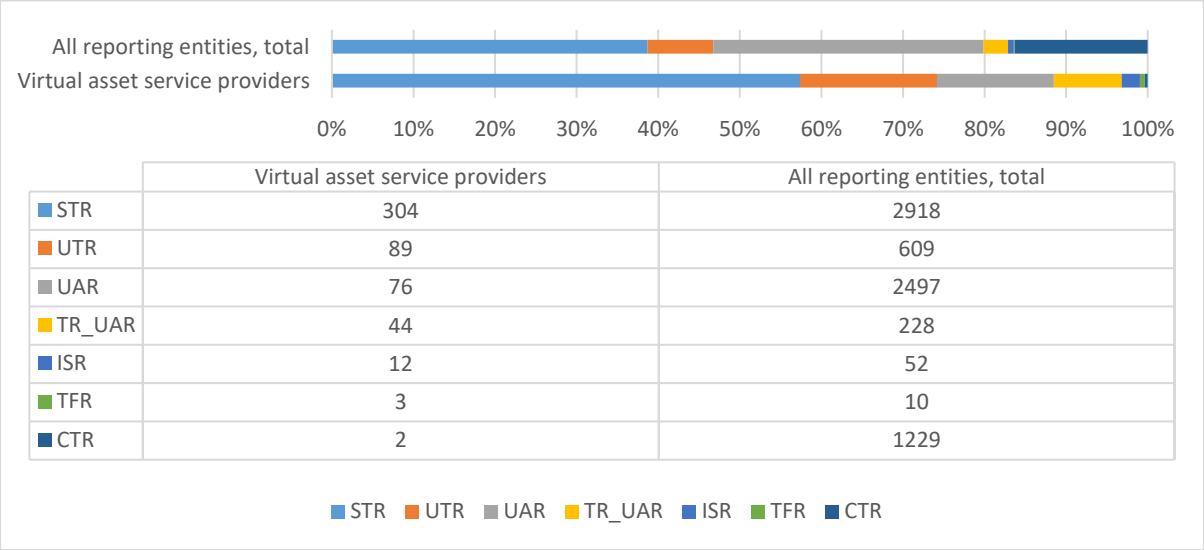
Table 1. Distribution of reports sent to the FIU in 2020 by groups.

Reporting group	Total
Credit institutions	4,594
Financial institutions	1,524
Agencies and persons from other countries	587
Virtual currency service	530
Professionals (legal, audit, etc.)	307
Public agencies	284
Non-obliged subject	252
Gambling operators	118
Other private entities	94
TOTAL	**8,290**

The largest proportion of the reports sent by virtual currency providers were related to money laundering: 304 Suspicious Transaction Reports (STR), 89 Unusual Transaction Reports (UTR) and 76 Unusual Activity Report (UAR) were submitted. In total, 47 terrorism-related reports were submitted, the majority of them, 44, were Unusual Activity Reports with reference to a high-risk country (TR_UAR) and 3 were Terrorist Financing Reports (TFR). For the first time, virtual currency service providers also submitted International Sanctions Reports (ISR;

[1] As at 1 April 2021

total 12). In 2020, two Currency Transaction Reports (CTR) were submitted by virtual currency service providers.



	Virtual asset service providers	All reporting entities, total
STR	304	2918
UTR	89	609
UAR	76	2497
TR_UAR	44	228
ISR	12	52
TFR	3	10
CTR	2	1229

Figure 1. Distribution of reports sent by virtual currency providers and all reporting entities to the FIU in 2020 by report types.

Similarly to 2019, the most frequent reason noted for submitting a report was that there are doubts as to the truthfulness of the data submitted by the person (1.2. STR). The reasons following in frequency are unusual transactions or unusual transactions with virtual currencies (2.3. and 4. UTR) or that an obliged person refuses to enter into a customer relationship with the person due to the impossibility to comply with due diligence measures (1.3. STR).

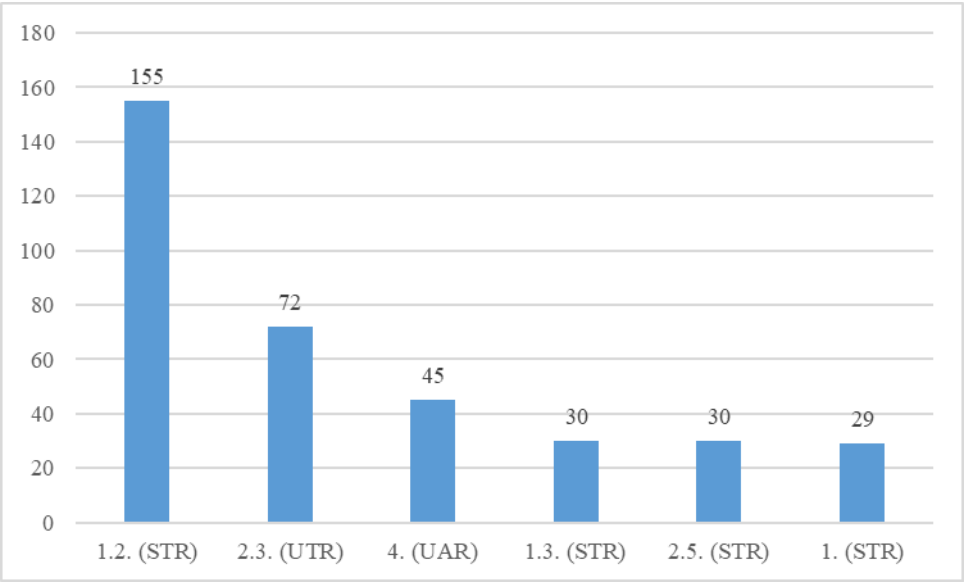


Figure 2. The most common indicators on the reports sent by virtual currency service providers to the FIU in 2020.

1.2. (STR) Doubts as to the truthfulness of the data submitted by the person
2.3. (UTR) Unusual transaction in virtual currency
4. (UAR) Unusual transactions in virtual currency

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 MLTFPA due to the impossibility of performing due diligence measures
2.5. (STR)	A person does not provide sufficient explanations or documents about the transaction to the extent necessary to perform due diligence measures or the submission is not plausible (MLTFPA § 42 (1) occasional transaction and § 43 (1) transaction of a person in customer relationship)
1. (STR)	At the time of establishing a business relationship / entering into a contract with a customer

Of the reports submitted by virtual currency service providers in 2020, 10 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.

Here, it is important to emphasise that reports not subject to in-depth analysis might also be important as they often become relevant over a longer period of time and are used to prepare strategic analyses of the typologies and trends in the sector.

In the materials sent to Estonian investigative bodies, the data contained in 49 reports were used, representing a significant increase compared to the previous year when the content of only two reports was forwarded. Through cross-border dissemination (XBD), information from 14 reports was shared with foreign countries.

The quality of the reports, and recommendations for the future

The quality of the reports submitted by virtual currency 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 often unjustified indication “urgent” on the report, especially where the customer relationship had been abandoned or the transaction had already been executed. It is also commendable that, compared to previous years, the majority of reports have been submitted via the online form. About 10% of the reports were still sent by e-mail. However, pursuant to § 50 (2) of the MLTFPA, reports should be submitted via the online form or via the X-road service.

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. It appears that the origin of the assets is often not identified and that transactions (including the origin of the assets from mixed sources) are not sufficiently analysed, not to mention displaying such information in the reports. The fact that a few major reporting entities are also monitoring transactions related to dark web environments is to be welcomed, as the FIU expects a similar approach from all market participants.

The FIU draws the attention of the service providers of the sector to the new trend that persons specialising in professional money laundering will also be emerging among virtual currency service providers[2]. We also suggest paying more attention to the ATMs of virtual currencies,

[2] https://www.zdnet.com/article/270-addresses-are-responsible-for-55-of-all-cryptocurrency-money-laundering/ and https://blog.chainalysis.com/reports/cryptocurrency-money-laundering-2021

which are increasingly more used in money laundering schemes, including in trade-based money laundering[3].

Conclusions from the monitoring proceedings of the FIU

In the 13 monitoring proceedings conducted for virtual currency service providers in 2020, the FIU identified shortcomings mainly in the application of due diligence measures and data storage. The monitoring showed that the obliged entities in the sector do not correctly verify the identity of a person involved in the transaction, i.e. the information provided by the customer is not verified from reliable and independent sources. In particular, this concerns transactions carried out remotely, where the customer's original document cannot be consulted directly. At least two different sources must be used here to verify the information. The FIU points out that a reliable and independent source is information (a) issued by (in the case of personal identification documents) or obtained from a third party who has no interest or involvement in either the customer or the obliged entity, i.e. is neutral; (b) for which there are no objective impediments to the determination of its reliability and independence, and the reliability and independence are also evident to a third party not involved in the business relationship; (c) in which the data present or obtained through it are up-to-date and relevant and the obliged entity is able to ascertain it.

In addition, in the course of monitoring proceedings, the FIU has identified shortcomings in the provision of information concerning a politically exposed person, his or her family member or a person known to be close associates of such person. For identifying such persons, virtual currency service providers use databases for which it is unknown how reliable these are in finding a match for a politically exposed person, his or her family member or a person known to be close associates of such person, and which exclude an easily applicable due diligence measure – customer questionnaires.

As regards data storage, virtual currency service providers often fail to maintain copies of documents submitted for identification and the correspondence held with the customer during the performance of due diligence measures. It is also a major concern that virtual currency service providers do not properly monitor their business relations. We emphasise that the rules of procedure and internal regulations must be in line with the requirements provided in law and with the activity of the market participant. Also, the contact person must be sufficiently competent to carry out his or her work duties. The FIU has encountered problems in communicating with some service providers where the contact person has not spoken either Estonian or English.

[3] https://www.theblockcrypto.com/linked/96962/crypto-atms-dea-report-money-laundering https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf