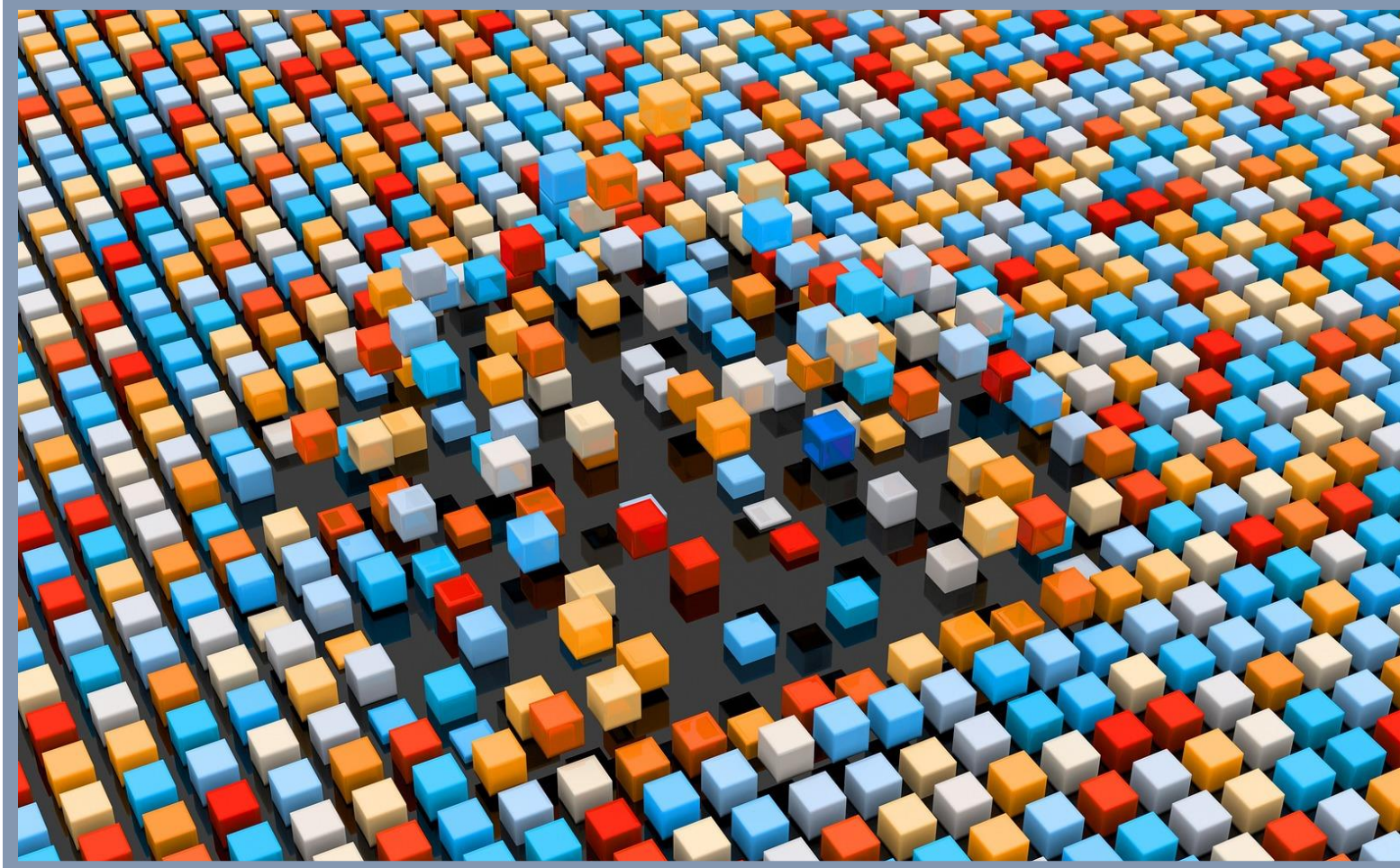
REPUBLIC OF ESTONIA
FINANCIAL INTELLIGENCE UNIT

THE RISKS RELATED TO VIRTUAL ASSET SERVICE PROVIDERS IN ESTONIA



January 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

INTRODUCTION 7

1. THREATS – TRENDS AND TYPOLOGIES 9

2. VULNERABILITY 13

2.1. VOLUME OF THE FIELD OF VIRTUAL ASSETS, SERVICE PROVIDERS' CLIENTS AND THE DIRECTION OF TRANSACTIONS 2021 13
2.2. THE RELATIONSHIP BETWEEN VIRTUAL ASSET SERVICE PROVIDERS AND ESTONIA 18
2.3. COUNTERMEASURES. LEVEL OF DILIGENCE OF VIRTUAL ASSET SERVICE PROVIDERS 23
2.4. THE RESULTS OF THE SUPERVISION PROCEEDINGS, OF THE FINANCIAL INTELLIGENCE UNIT 25

The Financial Intelligence Unit is mandated by legislation to execute strategic analysis that treats the risks, threats, trends, patterns and practices of money laundering and terrorism financing (MLTFPA § 54 section 1 paragraph 2). This study is a result of a factual and data-based strategic analysis of the Financial Intelligence Unit.

EXECUTIVE SUMMARY

Many of the facts and risks detailed in this study do not apply to the majority of service providers. Most enjoy good relationships with Estonia, their business plans are understandable, their teams have sufficient experience and size, and their risks are adequately managed with risk control measures. Many are innovative in the rapidly developing world of virtual assets. They offer the Estonian state long and short-term income and other benefits. The Estonian state can focus on these possibilities in more detail.

Threats

- Most virtual asset transactions are made within the current legislation. However, recent studies (also known as typologies) and findings by international law enforcement institutions indicate that virtual currencies are increasingly being used for criminal activity. Criminals use virtual currencies for payments amongst themselves and to commit crimes (incl. (dark web) payments for drugs, credit card data, child pornography etc, to demand payments from the victims of ransom attacks and other forms of extortion and fraudulent schemes), to conceal any trace of illegal property or money laundering, finance terrorism or to develop weapons of mass destruction and evade international sanctions.
- The number of foreign requests received by the Financial Intelligence Unit (FIU) and the number of mutual legal assistance requests for fulfilment issued to the Police and Border Guard Board by the Office of the Prosecutor General related to virtual asset service providers (VASPs) licensed by Estonia is increasing. The foreign requests in 2021 predominately concerned the movement of property acquired through fraud, ransomware, drug crime etc. through VASPs licensed by Estonia. In the interests of proceedings, the FIU cannot reference all criminal activities and their severity. However, known cases are related to criminal activity with high turnover and concern many of the aforementioned threats. Based on the fact that turnover (i.e the value of the mediated services) of VASPs licensed by Estonia increased nearly eight-fold from July 2020 to July 2021, we expect a large increase in the number of such foreign and mutual legal assistance requests.

Number of virtual asset service providers in Estonia

- At the time of the completion of this study (31 December 2021), 381 valid licenses for the provision of virtual asset services had been granted in Estonia.
- Unofficial statistics from mid-2021 indicated that nearly 55% of all global VASPs were registered in Estonia.
- As of July 2021, 253 VASPs licensed by Estonia were active. This is based on FIU survey data, with qualifying criteria of a minimum turnover from mediated virtual asset services of 2 000 euro between the period July 2020 to July 2021.

The volume of virtual asset services in Estonia

- The 253 actively operating VASPs licensed by Estonia have 4.8 million clients, of which 2 million are active. This number has increased nearly 4.5 times compared to 2019.
- The combined turnover of these 253 actively VASPs was 20.3 billion euro (from July 2020 to July 2021), and the total number of transactions was 66.3 million.
- Virtual asset services are clearly concentrated in the hands of a few large service providers (based on turnover and clients). More than 85% of this (17.7 billion euro), was generated by 15 service providers (during the period July 2020–July 2021).

Estonia's relationship with licensed virtual asset service providers

- 170 companies of the 253 actively operating VASPs licensed by Estonia, paid in the period 1.01.2020–30.09.2021 state and employment taxes in Estonia (approx. 2/3). The total amount within the 21 month period was 8.6 million euro, i.e. the average tax amount per month per company was 2 400 euro.
- The 15 largest (based on turnover) VASPs licensed by Estonia, have 2/3 of clients in Europe, just over a fifth in Asia (7% in Russia), 6.5% in North America, 3.5% in Africa, 2.5% in South America and 0.5% in Oceania. There are 0.6% (approx. 13 500) Estonian clients. The beneficial owners of more than a quarter of the clients (27%, approx. 550,000), do not include a single European Union (EU) resident.
- About 5/6 of the VASPs licensed by Estonia, have among the valid relationships in the Business Register, only one person with an Estonian background (Estonian personal identification or registry code). Less than a tenth of the VASPs are clearly related to citizens or companies registered in Estonia, i.e. the majority of the persons connected with the company are Estonians or Estonian companies, among the related persons of which the majority are Estonian residents.
- 44% of the VASPs have among the related persons at least one former or current e-resident.
- Nearly 75% of the companies licensed by Estonia for offering virtual asset services have among the related persons a corporate service provider (CSP). The providers of corporate services and legal services offer a part of the market participants thus the service of a nominal director.
- The majority of VASPs do not have a payment account in an Estonian payment or credit institution and they are serviced by Lithuanian payment and e-money institutions.

- A weak connection with Estonia is also referenced by the analysis of the seat addresses: approx. 2/3 of the VASPs licensed by Estonia, were initially registered merely to four addresses in Tallinn.
- The VASPs licensed by Estonia predominately have 1–2 employees or no employees at all in Estonia, incl. those service providers with a turnover of hundreds of millions of euro. This clearly indicates that the business system of the majority of market participants do not consider the expenses of the monitoring system and persons executing supervision or are outsourcing the identification service of persons. Many of the VASPs consider the contact person a formal obligation required by the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) that is also confirmed through the circumstances that one and the same contact person is associated with a highly disproportionate number of companies.

The level of diligence of virtual asset service providers

- Applicants for license of a VASP include a significant number of those who do not meet the requirements of the MLTFPA § 72 (they have not been licensed): these people lack an impeccable business reputation (e.g. they have been involved in bankruptcy proceedings, as a suspect or accused in criminal proceedings, there is concerning them negative information in public sources) or they have presented the FIU false information about themselves.
- Nearly 75% of the actively operating VASPs licensed by Estonia (253 in total) did not send a single report about suspicious transactions to the FIU in 2021.
- The due diligence measures of the vast majority of VASPs, at the time of establishing the client relationship nor during its duration, are in correspondence with the risks, size of the client base nor the volume of services provided. The majority of the VASPs licensed by Estonia lack efficient surveillance and monitoring systems that consider the specifics of the field of activity that would allow for the timely identification of transactions suspected of money laundering or terrorism financing. The supervisory inspections of the FIU have identified numerous weaknesses in procedural rules and risk assessments, due diligence procedures not being correctly applied, the politically exposed persons and beneficial owners have not been correctly identified etc.
- The offering of nested services that is essentially a correspondent relationship, significantly amplifies risks, as concealed behind a single client "account", maybe thousands and hundreds of thousands of subsequent clients, the identification and transaction monitoring of which, are not in the capacity of the local service provider.

Summarising conclusion

The application of due diligence measures of the majority of service providers licensed by Estonia is significantly insufficient compared to the volume of services offered, the weak level of AML/CTF, and skills and knowledge of the employees responsible for financial sanctions that all continue to reference high risks in the field. The requirement of proving the origin of property and/or wealth that is one of the important factors allowing for money laundering is frequently violated. There is a high risk that a weak level of application of due diligence measures by VASPs that anonymity permitting virtual currencies will be used for criminal purposes, incl. money laundering and terrorism financing.

The information collected domestically by law enforcement institutions, as well as the increased number of foreign requests and mutual legal assistance requests, related to

VASPs, references a continuing and continually increasing threat of using virtual currencies in criminal activities, incl. money laundering and terrorism financing.

The relationship of VASPs licensed by Estonia, with Estonia is weak. The analysis indicates that the legislative amendments made in 2020 did not fulfil their purpose: fulfilment of the requirement of a contact person and place of activity in Estonia, is viewed as a formal obligation by a large proportion of market participants, many operate at the same address and use the same contact person and the persons that companies present as contact persons do not correspond with the requirements of the legislation. The majority of them have only a few employees, if any, in Estonia. The client base consists of a marginal share of Estonian clients. A large proportion has among associated persons, only one Estonian resident, to fulfil the requirements of the legislation. Local providers of legal and corporate services are used for creating a formal connection with Estonia. The values of transactions among Estonian VASPs themselves are modest.

It is more complicated or practically impossible to execute supervision proceedings in cases where the employees of the VASP are not located in Estonia and also the victim(s) are not located in Estonia, and the service provider being merely formally connected with Estonia. The conducting of criminal proceedings could also be complicated in such an environment if money laundering or terrorism financing is committed through a service provider.

The requirements stipulated in the MLTFPA are not adequate if the state cannot actually verify the fulfilment of the given requirements and react upon identifying violations. The aforementioned leads to a situation in which the Estonian state currently predominately bears a reputational risk.

Many of the facts and risks presented in the study do not apply to many of the service providers – they are strongly related to Estonia, their business plans are understandable, they have hired teams of sufficient experience and size and use adequate risk control measures to manage risks. Many are innovative in the rapidly developing world of virtual assets, and in the long and short term provide the Estonian state, income and other benefits. The Estonian state can precisely focus more on these possibilities.

INTRODUCTION

Virtual asset service providers (VASPs) are people who offer (according to the Money Laundering and Terrorist Financing Prevention Act (hereafter *MLTFPA*[1]) § 3, 10 and 10[1]):

- a virtual asset wallet service or a service framework in which encrypted keys are created that can be used to maintain, store and transfer virtual currencies for clients;
- a virtual asset exchange service or a service framework in which a person exchanges virtual asset against cash, cash against a virtual currency or one virtual currency against another.

More than a decade ago, in 2008, VASPs were already subordinated to the regulations of the MLTFPA[2]. Estonia was one of the first countries in the world where this was done. A compulsory prerequisite for providing virtual asset services is licensing (MLTFPA § 70 (1)(4)). The FIU processes the applications for license and verifies the correspondence of activities of service providers with the requirements of the MLTFPA. The FIU has issued licenses to operate in the given field since 27.11.2017.

The national risk assessment (NRA) for AML/CTF, executed in 2020–2021 in Estonia, evaluated the risk level of VASPs in the field of money laundering as average (evaluation on a scale of 0–5 was 3, highest among the fields) and terrorism financing risk level as high (evaluation on a scale of 0–5 was 5, also highest among all fields evaluated in the NRA). The money laundering vulnerability level (4.02) and vulnerability level of terrorism financing (3.88), according to the NRA, are also highest for virtual asset service providers among all fields evaluated[3]. In the chapter on vulnerabilities in the field of financial engineering of the NRA[4], thoroughly exposing different threats and the probability of their realisation in Estonia is evaluated.

The FIU published the first in-depth risk assessment of money laundering risks related to virtual asset services in 2020[5]. The current study is a follow-up to this. The number of VASPs licensed by the FIU has noticeably decreased in recent years. It is thus time to update the risk assessment to obtain an overview of possible risk level changes in the field.

In the study, we used different data sources: the results of a survey conducted by the FIU among the providers of virtual asset services[6], data from the Business Register, Register of Economic Activities, Tax and Customs Board, Police and Border Guard Board and the FIU. An important resource in the study is the responses to a questionnaire that the FIU forwarded to market participants in the summer of 2021. All VASPs who had valid licenses at that time, including those who had temporarily withdrawn from economic activities, had to respond to

1 Money Laundering and Terrorist Financing Prevention Act. RT I, 17.11.2017, 2. RT I, 02.06.2021, 9.
2 They were at that time, a part of the alternative payment service providers that had an obligation of registration.
3 Estonian national risk assessment on the prevention of money laundering and terrorism financing 2020. Summary table. Ministry of Finance, 2021.
[https://www.rahandusministeerium.ee/system/files_force/document_files/1._kokkuvotte_tabel.pdf?download=]
4 Estonian national risk assessment on the prevention of money laundering and terrorism financing 2020. Vulnerability in the field of financial technology. Ministry of Finance, 2021.
[https://www.rahandusministeerium.ee/system/files_force/document_files/7._fintech_sektor.pdf?download=1].
5 Study on the providers of virtual currency services Financial Intelligence Unit, 2020. [https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee–accordion].
6 The FIU sent for obtaining the questionnaire, a precept to the service providers, for presenting the relevant data.

the questionnaire. The following information was collected with the questionnaire: general company data, data of the virtual asset service(s), data since 01.07.2020 on clients according to residency who had used virtual asset services, data on clients with the largest turnover, data based on residency on turnover of the counterparties of providing exchange services to clients and data on the turnover of the provision of virtual asset service.

513 companies of the 603 questionnaire recipients responded to the FIU. 173 of them had not begun trading, 87 had low activity (isolated clients, transactions and value of brokered services - we use the term "turnover" - remained below 2 000 euro). They were not included in the data analysis. The analysis used the responses of 253 companies. 90 companies did not respond to the precept and repeated precept (i.e., remained unresponsive to the questionnaire), of which 37 held before the response deadline licenses that were declared void.

The internationally recognised risk assessment methodology consists of two parts: evaluation of threats and vulnerability that when viewed as a whole provide a picture of risk. A threat is defined as a situation, event or activity that may exploit the vulnerability and damage the system. Vulnerability is a weakness that could be exploited by the threat. The report is also defined according to the following: the first chapter focuses on the exploitation of virtual asset threats by criminals and the second chapter on the vulnerability in the Estonian context.

1. THREATS – TRENDS AND TYPOLOGIES

There are many reasons for using virtual currencies that comply with legislation and the majority of virtual asset payments are legal. The practice of international law enforcement institutions, however, indicates that virtual currencies are increasingly used for criminal purposes; to commit different crimes (e.g., buying drugs from the dark web, ordering a cyberattack etc.) and to hide the tracks of property acquired through crime (e.g., ransom acquired through extortion, sale of drugs[7] or weapons on the dark web). It is possible to order almost anything with cryptocurrency from the dark web: drugs, murders[8], firearms, child pornography[9,10], deepfake, extortion[11], credit card data (in 2020 alone, the data of 115 million bank cards[12] were released), usernames, passwords, and much more.

In its analysis[13], Chainalysis, one of the best-known cryptocurrency transactions and blockchain analysis platforms, evaluated that the majority of crimes connected with cryptocurrencies are frauds. In 2020, there were cryptocurrencies to the value of approximately USD 2.6 billion connected to them as well as dark web marketplaces with associated transactions of an approximate value of USD 1.7 billion. The same trends are confirmed by an analysis of another well-known blockchain platform, CipherTrace[14] that highlights that soon the risk of using decentralised financing (DeFi) in money laundering will also increase due to the large flood of attacks.

It was highlighted in the introduction that fraud is growing rapidly in the world. Telephone fraud has also become a daily occurrence in Estonia and is consistently reported in local media publications. A subtype of telephone fraud is bank employee fraud where the fraudster acts as a bank employee. Data from the FIU show that property defrauded in this way is often converted into virtual currencies using payment institution accounts in Estonia. Fraudsters in recent times have also asked victims to deliver cash to cryptocurrency ATMs. Investment fraud is another widespread subtype of fraud where investment directly into cryptocurrencies or their derivatives is offered. Fraud has become industrial where criminals have an established division of work tasks, processes, task automation, client databases, performance indicators etc.

---

7 The Global Drugs Survey published in 2020, 9 analysis on different drugs that highlighted that constantly and in a growing trend (4.7% in 2014 and 15% in 2020), dark web marketplaces where payment takes place in cryptocurrencies, are used for obtaining drugs.
Source: Global Drugs Survey. 2020. Key findings. [https://www.globaldrugsurvey.com/wp-content/uploads/2021/01/GDS2020-Executive-Summary.pdf]
8 Dark web hitman identified through crypto-analysis. europol, 7.04.2021. [https://www.europol.europa.eu/newsroom/news/dark-web-hitman-identified-through-crypto-analysis]
9 4 arrested in takedown of Dark web child abuse platform with some half o million users. europol. 3.05.2021. [https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuseplatform-(s)-2-(2-chloro-4-chloro-2-chloro-4-chloro-5-
10 Sullivan, A. Dark web child porn bust leads to 338 arrests worldwide. Reuters. 16.10.2019. [https://www.reuters.com/article/us-usa-crime-exploitation-idUSKBN1WV1WW]
11 Bracken, B. Deepfake Attacks Are About to Surge, Experts Warn. Threatpost, 3.05.2021. [https://threatpost.com/deepfake-attacks-surge-experts-warn/165798/]
12 Gemini Annual Report 2020: COVID-19 Shakes Up the Carding Market. GEMINI Advisory. 17.12.2020. [https://geminiadvisory.io/gemini-annual-report-2020/]
13 The 2021 Crypto Crime Report. Everything you ned to know about ransomware, darknet markets, and more. Chainalysis, 16.02.2021. [https://go.chainalysis.com/2021-Crypto-Crime-Report.html]
14 Cryptocurrency Crime and Anti-Money Laundering Report. CipherTrace, Feb 2021, [https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/]

The 2020 European Cybercrime Centre (EC3), Internet Organised Crime Threat Assessment (IOCTA) - as one of the three drivers and challenges of criminal activity - highlights that virtual currencies continue to be (ab)used in all fields of cybercrimes, whereby development is directed towards cryptocurrencies and services oriented to privacy[15]. In the 2021 IOCTA[16], it is also stressed that increasingly anonymous cryptocurrencies are used on the dark web. In ransomware attacks and other extortion, criminals demand payment in virtual asset, because of the trustworthiness of virtual currencies, the non-reversibility of transactions and the perception that this is a method of payment with a high level of anonymity. Criminals also use virtual currencies on the dark web for transactions among themselves[17].

According to the IOCTA, the police are most frequently addressed in connection with extortion. Furthermore, in recent years, the number of ransom attacks in which criminals demand that victims pay them in virtual assets (mostly in Bitcoin) has been on an increase in Europe. It would not have been possible to conduct large ransom attacks in recent years without cryptocurrency as bank transfers and cash do not offer sufficient opportunities for a rapid onward payment and hiding the tracks of ransom payments.

Virtual currencies are not solely used for committing crimes and hiding the tracks of criminal property in money laundering but also for financing terrorism and evading international sanctions. Means are often collected as donations for financing acts of terrorism or terrorist organisations. Transactions to risky countries and regions are filtered out by banking systems. Furthermore, virtual currencies are increasingly used to collect means. Terrorist organisations may collect support under the cover of humanitarian aid but also directly to support their worldview or a clear purpose of use, such as the acquisition of some weapon[18,1920]. There are also examples of donations collected in virtual currencies by right-wing extremists[21.22]

Law enforcement institutions have identified many cases where cryptocurrency acquired with different criminal offences has been used to evade international sanctions and finance the development of weapons of mass destruction. Many sources reference hackers associated with the government of North Korea who have used cryptocurrencies acquired

15 Internet Organised Crime Threat Assessment 2020. europol, 2020, [https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020].
16 Internet Organised Crime Threat Assessment 2021. europol, 2021, [https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021]
17 Internet Organised Crime Threat Assessment 2020. europol, 2020, [https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020].
18 O'Leary, R.R. Wired. The bitcoin terrorists of Idlib are learning new tricks. 31.03.2021, [https://www.wired.co.uk/article/bitcoin-crypto-terrorism-syria]
19 Funding terrorism: campaign of a jihadi organization operating in the Gaza Strip to raise funds in Bitcoin. The Meir Amit Intelligence and Terrorism Information Center. 19.05.2019. [https://www.terrorisminfo.org.il/app/uploads/2019/05/E_109_19.pdf]
20 Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. US DOJ. 12.08.2020. [https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns]
21 Bogle, A. Buying and selling extremism. Australian Strategic Policy Institute. 19.08.2021. [https://www.aspi.org.au/report/buying-and-selling-extremism]
22 Andrews, F., Pym, A. The Websites Sustaining Britain's Far-Right Influencers. Bellincat, 24.02.2021. [https://www.bellingcat.com/news/uk-and-europe/2021/02/24/the-websites-sustaining-britains-far-rightinfluencers/]

through theft from financial institutions and different ransom demands in the development programmes of nuclear weapons and launchers[23,2425].

The role of VASPs is expected to increase in the upcoming years in the prevention of financial sanctions evasion and developments of the US OFAC sanctions, developments of sanctions in different countries, and in associations of groups of countries. The FIU sees the threat despite monitoring service providers (Chainalysis, CipherTrace, Coinfom etc.) developing systems to assist in identifying sanctioned persons. It's evident that providers of virtual asset services will not be capable of effectively preventing the evasion of financial sanctions if their capacity in the application of "know your client" and due diligence measures do not increase.

It is difficult to detect where the activity actually takes place in the case of companies that are associated with different jurisdictions (e.g., if a company established in an *offshore* area is licensed by Estonia but clients are, for example, predominately in Ukraine or Russia and IT support is offered by a company from a third country). The same applies to groups of companies where different activities are distributed between different companies making it difficult for clients to understand with which company the actual contractual relationship is formed.

The connection with Estonia for many companies licensed by Estonia is weak (there are few employees in Estonia, little taxes are paid etc., see more in Chapter 2.2) and activities take place elsewhere. The FIU established that a significant proportion of virtual asset services providers licensed by Estonia have a connection with Russia and Ukraine. That is, persons connected with the companies have a Russian or Ukrainian background. However, connections also become apparent from cryptocurrency and *fiat transactions* as the dominating currencies of these companies are the UAH (Ukrainian hryvnia), USD (US dollar) and RUB (Russian rouble).

Ransom attacks, telephone fraud, malware attacks and other crimes where virtual currencies are used, connection is often made with hackers speaking Russian as their native language. The "melting" of criminal property also takes place in Ukraine, Russia and the Middle East. In the second-tallest office building in the world, Federation Tower East (Vostok) in Moscow, there are at least a dozen active VASPs associated with "melting" property that was acquired from ransomware attacks and other crimes[26], with many more in the area.

---

23 Analysis: How Chinese Nationals Linked to North Korea Laundered Hundreds of Millions of Dollars' Worth of Stolen Cryptocurrency Through Several Banks and Cryptocurrency Exchanges. CipherTrace. 12.03.2020.03.12. [https://ciphertrace.com/chinese-linked-dprk-laundering-analysis/.]

24 Lederer, E.M. UN experts: North Korea using cyber attacks to update nukes. APNews, 10.02.2021. [https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4844780f54a3279ef707b33]

25 Nichols, N. North Korea took $2 billion in cyberattacks to fund weapons program: U. N. report. Reuters, 5.08. 2019.08.05. [https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX]

26 Ransomware HQ: Moscow's Tallest Tower Is a Cybercriminal Cash Machine. Bloomberg, 03.11.2021. [https://www.bloomberg.com/news/articles/2021-11-03/bitcoin-money-laundering-happening-in-moscow-s-vostok-tower-experts-say]

At times, there have also been VASPs on the OFAC sanctions list that have operated in Russia and been connected to companies licensed by Estonia. This is a significant risk to Estonias' reputation.

In autumn 2021, the FIU voided the license of Company A to offer virtual asset services. Company A, according to public sources, had given notification of a temporary withdrawal from economic activities on 30.06.2020 and was closely connected with, amongst others, the cryptocurrency exchange platform operating under the Chatex trademark. Chatex tried to give the public the impression that it had been licensed to offer virtual asset services in Estonia and indicated on its website that it was operating on the basis of the license issued to Company A. The FIU is of the standpoint that it is not allowed to "lend" a license issued in Estonia. Only the person to whom the license has been issued may operate on its basis.

2. VULNERABILITY

2.1. VOLUME OF THE FIELD OF VIRTUAL ASSETS, SERVICE PROVIDERS' CLIENTS AND THE DIRECTION OF TRANSACTIONS 2021

Among the 30 largest VASPs in the world, not a single company is licensed by Estonia[27]. The largest market participant in the entire world, at the end of December 2021, was Binance which had a daily transaction volume of USD 14 billion or in total for 2021, USD 7.7 trillion[28].

The application for licenses to offer virtual asset services gained momentum in 2017 in Estonia when the corresponding regulation in the MLTFPA came into force. In 2017-2019, there was a rapid increase in the licenses for virtual currencies; there were a thousand or more licenses issued per year (Table 1). The momentum gain in the number of licenses was accompanied by a rapid escalation of risks and the FIU saw that the requirements presented for applying for licenses for VASPs did not allow mitigation of the risks. The possibilities for the FIU at that time, for refusing to grant a license, connected with offering virtual asset services were scarce because, in principle, the only basis of refusal was a criminal punishment of the persons connected with the company.

In 2020, the FIU executed the first in-depth risk assessment in the field of VASPs for which data was also collected in 2019 from market participants in the form of a questionnaire[29]. The results of the survey indicated that many of those licensed had not commenced activities within six months of being granted license and the FIU voided their license. This was the main reason why the number of licenses declared as void rose sharply in 2020 in comparison to the two previous years. Another reason was the version of the Money Laundering and Terrorist Financing Act that had come into force in March 2020 that established stricter requirements for VASPs in applying for licenses. Companies had to correspond with the new requirements by 01 July 2020 at the latest. The licenses of companies that did not fulfil the given requirements were declared void by the FIU within the second half of 2020. In September 2021, there were approximately 400 companies in Estonia with an active issued license (i.e., not temporarily suspended by themselves etc.) to offer virtual asset services (Table 1). According to informal statistics, 54.8% of all of VASPs in the world were registered in Estonia as of mid-2021. 15 new license applications were presented on average in 2021 to offer virtual asset services (181 in total in 2021). At end of December 2021, there were 180 active license applications for virtual currencies (applications for amendments and new applications).

27 Coinmarketcap data as of 31.12.2021, [https://coinmarketcap.com/rankings/exchanges/]
28 Coinmaketcap data as of 31.12.2021, [https://www.businessofapps.com/data/binance-statistics/]
29 The methodology of the study, is described in the 2020 study report, of VASPs that is also published on the website of the FIU: [https://fiu.ee/media/68/download]

Table 1. Overview of activity licenses to offer virtual asset services 2017-2021

	27.11.2017–31.12.2018	1.01–31.12.2019	1.01. –31.12.2020	1.01–30.12.2021
Active licenses*	603	1234	473	381
Licenses declared void	37	97	1808	329
New licenses	1130	1305	325	86

* Concerned at the end of the period, are licenses issued by the FIU to offer virtual asset service

Source: FIU

The results of the survey conducted in summer 2021 show that VASPs licensed by Estonia offer mainly three services. Of the253 active companies that responded to the questionnaire, 92% (233 VASPs) reported that they offer a service to exchange virtual currency for cash, 61% (155 service providers) offer a virtual currency wallet service, 55% (139 service providers) offer a service to exchange virtual currency against another virtual currency, five offer a service of cryptocurrency payment card service and two a crypto ATM service.

The number VASPs clients increased approximately 4.5 times during July 2020-July 2021[30] in comparison to 2019 when the FIU first collected data to evaluate the volume of the field of virtual asset, [31] according to data reported by the companies. It must thereby be taken into consideration that the number of companies whose data forms the basis of the given evaluation, decreased by 27. The 253 VASPs (i.e., actively operating companies licensed in Estonia for virtual asset services) that had responded to the questionnaire had a total[32] of 2 million active clients[24] from July 2020 to July 2021[33]. The number of clients of VASPs varied within very large ranges starting from one client to more than 350 000 active clients. From July 2020 to July 2021, the service providers that responded to the questionnaire had a total of 4.8 million clients (i.e., active and passive). The companies had defined approximately 200 000 clients with a higher risk of money laundering. Almost 550 000 clients (or about 27% of all clients) had non-EU residents as their beneficial owners, i.e., outside the EU (including the United Kingdom).

The total number of transactions for the 253 active companies in the field of virtual asset services that responded to the questionnaire was more than 66.3 million (i.e., on average, 262 000 per company) and a turnover[34] of 20.3 billion euro (i.e., an average of 80 million euro per company). For comparison, in the first half of 2019, the turnover of the 280 virtual asset service providers that responded, according to the data presented to the FIU, was 1.2 billion euro in total. In other words, the turnover of virtual asset services of companies licensed by Estonia increased during July 2020-July 2021 approximately 8.5 times compared to 2019[35].

30 Study of the providers of virtual currency services Financial Intelligence Unit, 2020. [https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee—accordion]

31 We use here in the interest of simplicity the term "client". It includes those persons with whom has been created a business relationship, as well as those with whom the VASP has executed occasional transactions. An occasional transaction is such a transaction that is so to say outside a business relationship, i.e. does not create a client relationship. The number of clients using the infrastructure of service providers may be significantly higher, as it is possible that nested services might be used.

32 Those companies were not included in the 2021 analysis that had a turnover of less than 2 000 euro.

33 We are in the interest of simplicity calling the period of observation "July 2020–July 2021", but in reality it was offered to the respondents of the questionnaire to present data starting from 1.07.2020 up to the time of completing the questionnaire. The most recent responses were presented to the FIU at the end of September 2021.

34 The term "turnover" is used to of the value of the mediated services.

35 The FIU in the 2020 questionnaire, requested information on turnover, related to the virtual currency services of the I half year of 2019. We have assumed in comparing the turnover of the two periods (July 2020–July 2021 vs. 2019) that the turnover in the second half of 2019 was comparable to that of the first half year.

The turnover of the cryptocurrency payment card services was approximately 13.5 million euro and 0.5 million euro for crypto ATM services.

The field of virtual asset services based on turnover and clients is concentrated in the hands of a few large service providers. More than 85% of the turnover (17.7 billion euro) in July 2020-July 2021 in the field of virtual asset services was generated by 15 service providers. Of them, two reported virtual asset service turnovers above 5 billion. Only a few of the VASPs licensed by Estonia run their business for Estonian clients (the share of Estonian clients is 0.6%).

Estonia received tax revenue during 1.01.2020-30.09.2021 from 170 companies of the 253 active companies that responded to the questionnaire. The total amount for the 21 months was 8.6 million euro, i.e., an average of 2 400 euro per company. The 15 companies in the field of virtual asset services with the highest turnover, which totalled 17.7 billion euro according to the data presented to the FIU, thereby paid state taxes in Estonia in total 525 715 euro and labour taxes 460 690 euro during 1.01.2020-30.09.2021. In other words, approximately 1 million euro in taxes for 21 months. Two companies thereby paid 50% of the taxes. Two of the 15 companies did not pay any taxes in Estonia in the given period and the tax amount of one was marginal (less than 700 euro). The median tax amount of those companies that paid taxes, was 32 000 euro for the 21 months, i.e., about 1 500 euro per month. These 15 companies declared a total turnover in Estonia of 3.9 million euro with a taxable turnover of 3.5 million euro.

The data presented by the companies did not provide a reliable overview of the residency of the clients of the companies licensed by Estonia as the largest service providers left the residency of approximately half of the clients unspecified; these companies reported in general 2.1 million clients and residency data was presented for 1.05 million clients. Data is not collected for the remaining clients that the FIU considers worrisome from the standpoint of evaluating geographical risk. Also concerning these clients, due diligence measures that are proportionate to the risk are not applied. The presented data on client residency indicates that based on turnover, the 15 largest VASPs licensed by Estonia had mostly clients from Europe (slightly less than 2/3 of all clients). They are mostly residents of Poland, France and the United Kingdom. A bit over 1/5 of private clients reside in Asia (7% in Russia), 6.5% in North America, 3.5% in Africa, 2.5% in South America and 0.5% in Oceania. There were about 13 500 Estonian clients.

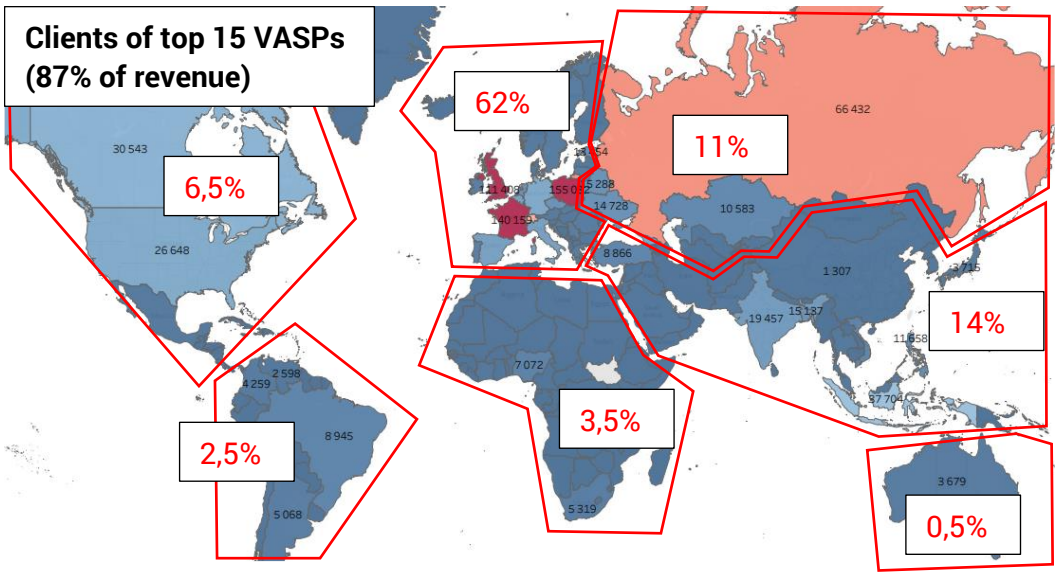


Figure 1. Residency of private clients of the 15 largest service providers by turnover (data for 1.05 million clients)

Regarding the provision of exchange services[36], the questionnaire sought to establish where property originates from (Figure 2, total 7.8 billion euro) and where it goes (Figure 3, total 6.5 billion euro) based on the residency of transactions' counterparties (virtual assets received by clients, virtual assets sent by clients). It is possible to generally observe that in the case of the 15 largest companies, there is a disproportionately large property going to Luxembourg, Syria, Pakistan, Greece, Montenegro, Serbia and Belize. Property thereby leaves mostly from Russia, Japan, Switzerland and North and South America.

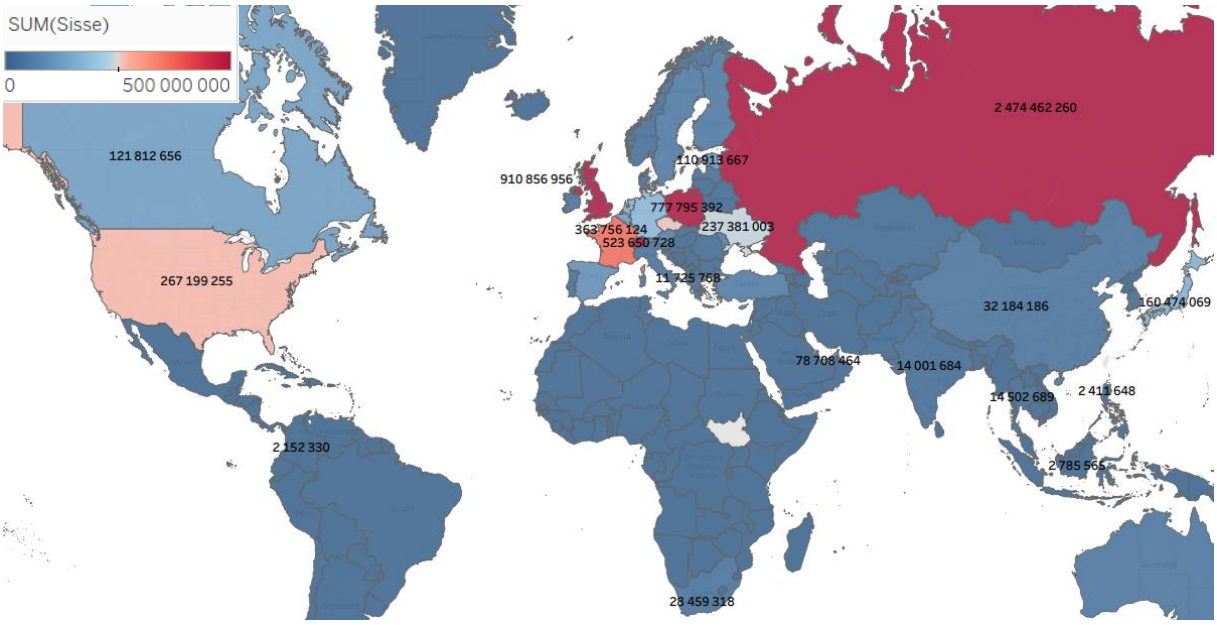


Figure 2. Origin of the currency received by the clients of the largest service providers (in euro; "sisse"= incoming)

36 Requests were about transactions with virtual currency against virtual currency as well as virtual currency against fiat currency.

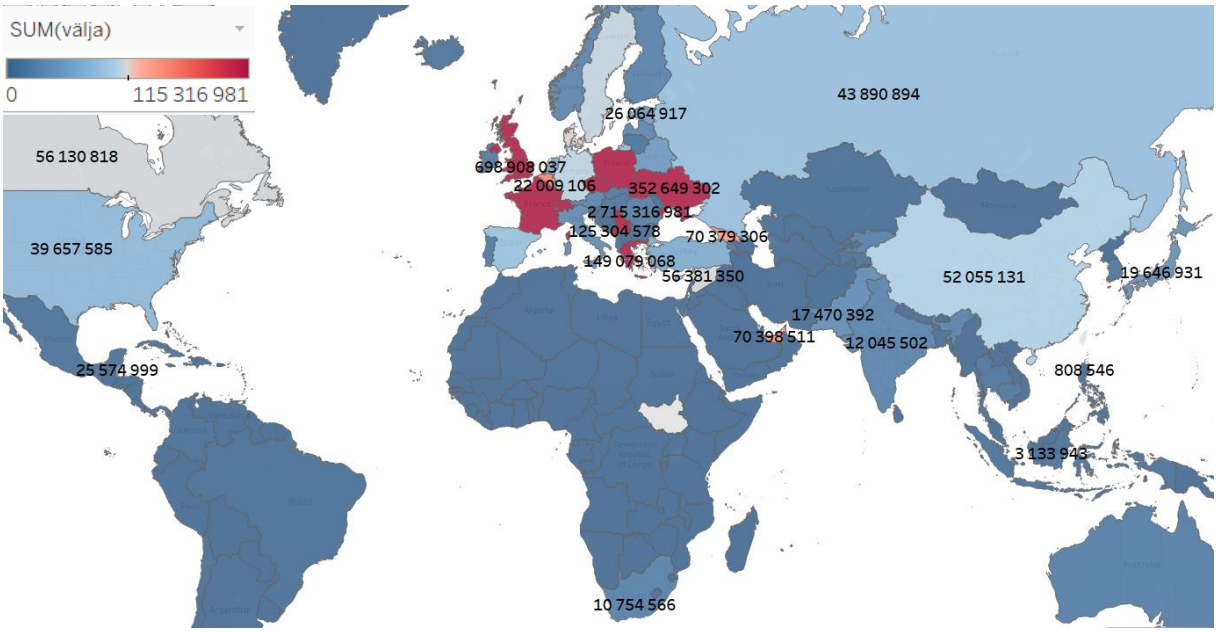


Figure 3. Currency (in euro) sent by clients of the largest service providers based on the residency of the counterparty ("välja"=outgoing)

The greater the geographic and linguistic distance with clients, the more difficult it is to know the client and detect suspicious and unusual transactions in his/her activities. In the case of clients that are non-resident legal persons, the application of know your client due diligence measures is also made more difficult if the corporate client has registered itself in one country and is active in (an)other countr(y)ies. It is also difficult if the transparency concerning companies and data of persons associated with them is poor in the jurisdiction of registration. There are different reasons for concealing oneself behind companies in these countries, e.g., optimisation of taxes, the speed or simplicity of founding a company, the desire to conceal or complicate the identification of the beneficial owner and their actual will, as well as clarifying the (illegal) origin of property.

The 15 VASPs with the highest turnover (in July 2020-July 2021) have clients throughout the world, many of them from more than 100 countries. These clients speak various native languages. Each country has a unique form of identity document. An efficient application of due diligence measures and effective risk management in the case of such a diversified client base assumes that companies are competent regarding such varied documents and client backgrounds to identify situations where attempts are made to use a false identity or forged documents. The analysis of the reports received by the FIU raises doubts about most of the companies licensed by Estonia as a VASP being capable of correctly identifying the identity of clients and suspicious transactions (for example, transactions with dark web service providers, mixers etc.) as well as manage their (operational) risks. However, the suspicion of using a false identity is the most frequent reason for sending a report (see Chapter 3), but service providers identify this mainly through facial recognition systems, the client's name or based on documents with obvious forged characteristics.

2.2. THE RELATIONSHIP BETWEEN VIRTUAL ASSET SERVICE PROVIDERS AND ESTONIA

A factor that raises the risk level of the field is also the lack or limited transparency of the management scheme of VASPs. In a study completed in 2021, the FIU highlighted that regarding the money laundering risks of CSPs[37], Estonian CSPs advertise Estonian virtual asset service license internationally as a quality label to service providers, allowing the service provider to confirm to clients that their property is in a secure location. Many of the local CSPs offer the service of preparing license for providing virtual asset services. Estonian companies that have a license service for virtual assets have become a sales article including for companies that offer international corporate services.

Approximately 5/6 of the VASPs licensed in July 2021 by Estonia to offer virtual asset services had only one Estonian person, either natural or legal (contact persons and founders that were often CSPs have been thereby excluded) among the valid associations in the Business Register (shareholders, members of the management board and supervisory board, beneficial owners). This scheme raises doubts about whether these companies have added an Estonian person to only formally fulfil the legal requirement, i.e., create a formal connection with Estonia. Such formal management members (including CSPs and providers of legal services) might not sufficiently know the business model or company owners, making it impossible for them to apply the required diligence. Under certain factual circumstances, this could lead to criminal liability (e.g., through assisting) if the company is used for criminal purposes.

Less than 1/10 of the VASPs are clearly related to persons with an Estonian personal identification or registry code, or the majority of persons connected with the company are Estonians or Estonian companies that have predominately Estonian residents.

44% of the VASPs have at least one former or current e-resident among the associated persons. The given indicator in 2020 was approximately a third[38], i.e., the indicator has increased by more than 10% over the year. Approximately, every tenth (10%), of all the persons connected with all of the VASPs licensed by Estonia, is an e-resident. The profile of the e-residents connected with VASPs is similar to the general profile of origin of e-residents (e-residents are mostly from Russia, Finland, Ukraine, Germany, China, the United Kingdom and France).

37 The money laundering risks associated with the providers of corporate services in Estonia. Financial Intelligence Unit, 2021. [https://fiu.ee/media/149/download]
38 Study of the providers of virtual currency service Financial Intelligence Unit, 2020, [https://fiu.ee/media/68/download]

Table 2. Overview of the countries of origin of e-residents connected with VASPs licensed in Estonia (countries from which at least six e-residents originate)

Country	E-residents
Russia	47
Latvia	44
Ukraine	33
Germany	13
Poland	12
France	11
Spain	9

Country	E-residents
UK	9
Italy	9
China	8
Romania	6
Israel	6
Canada	6

In the FIU study regarding the money laundering risks of CSPss[39], we also highlighted that Estonian CSPs offer the service of a fictitious place of activity to VASPs. The reason is an amendment to legislation enforced in March 2020 that led to an important change for VASPs, establishing the requirement of a place of activity in Estonia. With the establishment of additional stricter requirements, the legislation hoped to end allowing virtual asset services so that companies factually located in Estonia could offer the service without essential supervision (the service is not offered from Estonia nor to Estonian clients).

Nearly 5/6 of the VASPs with a valid Estonian license were initially registered to only four addresses in Tallinn (Table 3, data as of July 2021). There were around 1/4 of a hundred addresses that were recorded as the addresses of at least 10 VASPs.

Table 3. Overview of the most used initial places of activity of VASPs licensed in Estonia

Address (with exact building)	VASPs at the address
Tallinn, Väike-Paala tn 2/ Peterburi tee 47	226
Tallinn, Rännaku pst 12	92
Tallinn, Roosikrantsi tn 2	73
Tallinn, Punane tn 6	35

The FIU has also experienced fictitious business addresses when executing supervision checks; ie. the FIU has found that companies are not actually at the address they have presented to the FIU as their place of business and it was not possible to make contact with the company representatives at the given location.

Among others, CSPs also offer VASPs the service of a nominal board member and shareholder. Some law firms advertise the offering of such illegal nominal persons publicly on their websites. Nearly 75% of the companies that are licensed by Estonia to offer virtual asset services have a CSP among associated persons. These companies where the actual or beneficial owners use such "services" increase the level of risk of the field as they reference the offering of fictitious service.

39 The money laundering risks associated with the providers of corporate services in Estonia. Financial Intelligence Unit, 2021. [https://fiu.ee/media/149/download]

According to data from the Business Register, as of 30.09.2021, the 15 largest companies offering virtual asset services, by turnover (they all have a turnover of 100 million euro or more), had a total of 27 employees in Estonia (less than two employees per company on average). Such a small number of local employees in the context of such large turnover and volume of clients raises serious questions about whether companies contribute sufficiently to the control mechanisms. The 253 companies that reported to the FIU that they are actively in operation, when responding to the questionnaire, had, in the first three quarters of 2021, on average a combined total of approximately 320 employees in Estonia (i.e. an average of 1.2 employees per company). Such a low number of registered employees means that many VASPs may have serious problems in separating risk-taking and compliance control measures. It's not possible to fulfil the AML requirements and manage risks with two employees (even if the role of both employees are AML), as by nature in such a case there is a conflict of interest. There could also be security and sustainability problems in situations where one or both of these measures have been outsourced to third parties and the liability of the company has not been allocated (incl. at management board level).

From 2020, the FIU has, resulting from amendments to legislation, significantly supplemented its process of processing license applications, and the requirements for these licenses have become more thorough. The FIU verifies management board members, owners, beneficial owners and the contact persons of the applicant when granting a license to offer virtual asset services. The FIU, in addition to the criminal record certificate, also investigate their reputation, knowledge and experience in the given field, as well as if and how AML/CTF is ensured in the company. Their evaluations so far indicate that the majority of the companies that apply for licenses or amendments do not meet the requirements stipulated in MLTFPA § 72. Persons lack a proper commercial reputation (e.g. they have been participants in bankruptcy proceedings, are suspects or accused persons in a criminal proceeding or there is negative information about them in the public domain) and during the verification process, false information was presented to the FIU (information is concealed and withheld). Below is just one example of the many that the FIU has encountered.

> Companies A, B and C, in the process of applying for a license, submitted a CV from a board member that indicated that the person worked in AML in larger credit institutions. The named companies were granted licenses. When the FIU processed an amendment to the company's license later in 2021, they interviewed the board member, where it became apparent that the member lacked sufficient knowledge in AML and had never worked for the companies listed on their CV. The FIU retracted the licenses of the three companies (as they had presented false information at the time the licenses were granted). The FIU also reported it as a criminal offence.

Often, management board members associated with more than one VASP lack an overview or understanding of who the owners and beneficial owners of the company they manage are, how the business activities of the company function, and what their obligations in the company are. When responding to elementary questions about the company, interviewees have attempted to use other means to assist in answering the questions put to them. This indicates that the member concerned is a nominal person that is employed by the company to fulfil the legislative requirement that the management board must be located in Estonia. The company is actually managed from abroad and lacks any type of connection with Estonia apart from the legal "body" in the local register and the applicant's license. The company is

registered to an address to which are registered dozens or hundreds of other companies, owners and beneficial owners are foreigners, among the language selection of the website, Estonian is missing, payment accounts are abroad, important decisions are taken abroad etc. A significant number of VASPs, as described above, do not have employees in Estonia or there are 1-2 employees. These companies also do not pay any taxes at all in Estonia or the amount of taxes paid is modest. Many companies have admitted that the only reason they apply for a license in Estonia is that it's easy and economical to obtain. There are, of course, others whose activities in Estonia and the local license are clearly justified. They bring innovation into the country.

It has become apparent in processing license applications that persons employed as contact persons, do not correspond with the requirements stipulated in the MLTFPA. Their knowledge of AML/CTF is incomplete and the risks associated with virtual currencies are not known. Many of them have not become acquainted with risk assessments or the procedural rules of the company and do not know the requirements of applying due diligence measures. A significant part of them have a connection with Estonia that is merely formal, have an insufficient number of employees to ensure the prevention of money laundering, lack knowledge on compliance checks and audits and a business plan, or do not exist in reality. The FIU sees a risk in the insufficient knowledge of fulfilling the reporting obligation – what types of reports (STR, UTR, UAR, etc) exist, what characteristics they correspond to and how and when reports must be sent to the FIU. Contact people are not capable of naming the phases and characteristics of money laundering based on how to recognise suspicious transactions, terrorism financing or how and in what way to detect financial sanctions and avoid them. The given contact people also lack an overview of the technical means that the company uses in the execution of its due diligence measures and in monitoring transactions, and what their related processes are.

There has been an annual increase in the number of foreign requests from law enforcement institutions from other countries made to the FIU in connection with VASPs. In the first 10 months of 2021, the FIU received 100 such foreign requests, nearly a third more than the total for 2020. The contents of the foreign requests in 2021 have predominately been connected with the movement of property acquired as a result of fraud through VASPs licensed in Estonia. The foreign law enforcement institutions have also sent requests concerning virtual asset providers themselves and their related parties.

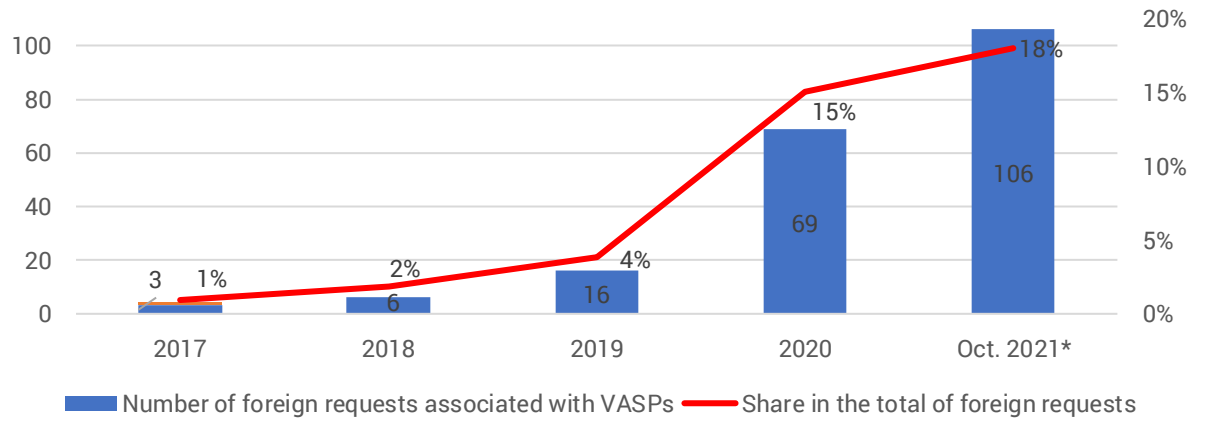


Figure 4. Number of foreign requests that the FIU has received in connection with VASPs 2017-2021

** As of 31.10.2021*

In the period 01.01.2019 to 30.08.2021, 126 mutual legal assistance requests from foreign law enforcement agencies regarding VASPs licensed in Estonia were received from the Office of the Prosecutor General for fulfilment by the Police and Border Guard Board (PBGB).

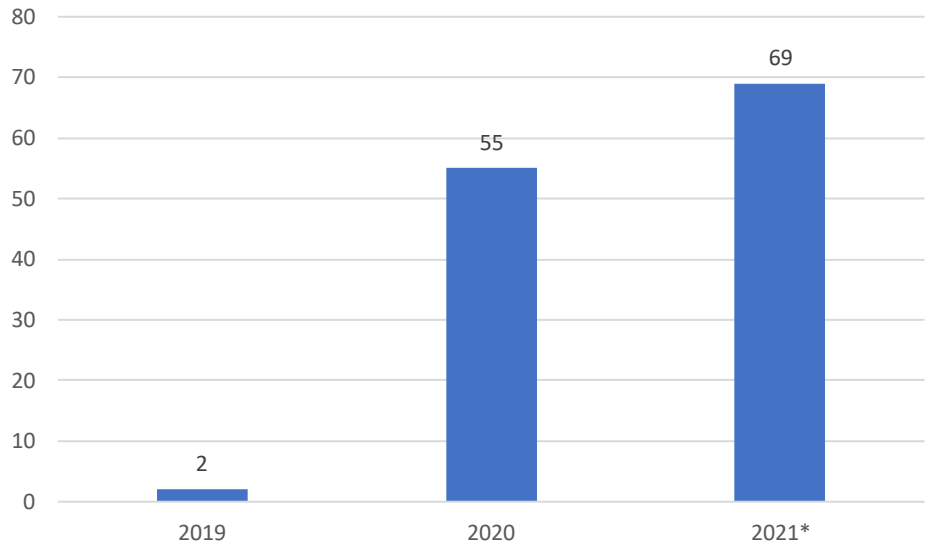


Figure 5. Number of mutual legal assistance requests in which the PBGB has made a request to a VASP licensed by Estonia, 2019-2021

** As of 30.08.2021. Source: PBGB*

Most of the mutual legal assistance requests received by the PBGB in connection with VASPs licensed by Estonia came from Poland, Germany and the USA. The alleged criminal activity in these queries has mainly been (cyber and computer) fraud.

A large portion of these foreign requests is connected with criminal cases that occurred a few years ago. It's expected that in the next few years, given that from July 2020 to July 2021 the turnover of transactions mediated by VASPs licensed by Estonia increased nearly eight times, there will be a noticeable increase in the foreign and mutual legal assistance requests connected with VASPs licensed by Estonia.

Foreign requests from 2021 predominately concern the movement of property acquired through fraud, ransom, drug crime etc., through VASPs licensed by Estonia. The FIU cannot in the interests of proceedings, reference all of the criminal activities and their extent, but can state that known cases are related to high-turnover criminal activities and are connected to many of the aforementioned threats that, according to international studies, increasingly involve VASPs.

2.3. COUNTERMEASURES. LEVEL OF DILIGENCE OF VIRTUAL ASSET SERVICE PROVIDERS

A person that has been granted a license must be capable of applying the due diligence measures stipulated in legislation, creating client relationships and notifying the FIU of suspicious transactions. Their technical solutions and knowledge of employees must be sufficient for monitoring clients and transactions.

The number of reports sent to the FIU by VASPs dramatically increased in the period 2017-2021. The number of reports sent in the first nine months of 2021 has exceeded double the number of reports sent in 2020. The number of reporters has also increased (Table 4).

Table 4. Reports sent to the FIU by VASPs, 2017-2021

	2017	2018	2019	2020	1.01.-5.10.2021
Number of reporters	1	4	16	45	62
Number of reports submitted	1	6	405	530	1100

Source: FIU

The increased number of reports sent and senders is positive but the content of the reports received in 2021 from VASPs continues to indicate that the level of due diligence of the vast majority of market participants in the field doesn't correspond with the risks. As can be seen in Table 4, in the first nine months of 2021, the FIU received reports from 62 VASPs. The data collected by the FIU indicate that there are 253 active service providers on the market, thus only about a quarter have sent reports. As of July 2021, almost 75% of the market participants licensed for virtual asset services that responded to the questionnaire and stated that they were active (i.e. that they had turnover in the period July 2020-July 2021) have not sent a single report to the FIU in 2021.

There is no correlation between the number of reports presented by the reporters and the total turnover related to virtual asset services. There are 9 companies among the TOP15 service providers, licensed by Estonia with turnover in virtual currencies that have (as of 17.11.2021) sent fewer than 6 reports in 2021, incl. among them, four that have not sent a single report; service providers that have presented only a few dozen reports have a significant turnover that in most cases amounts to tens or hundreds of millions. Most of the market participants that offer virtual asset services with a significant turnover of hundreds of millions and are licensed by Estonia have sent no or only some reports to the FIU in 2021.

The risk of VASPs, in addition to turnover, is also impacted by the geographical location of their clients. The client base and transactions of some of the service providers ranked in the top 15 by turnover are connected with regions to which it would currently be difficult to make or receive transfers, through credit institutions located in Estonia. The number of their presented reports, however, does not appear to be proportionate to the client base or the geographic risks of their executed transactions. This clearly points out that their due diligence measures do not correspond with the risk, size of the client base or the volume of services provided.

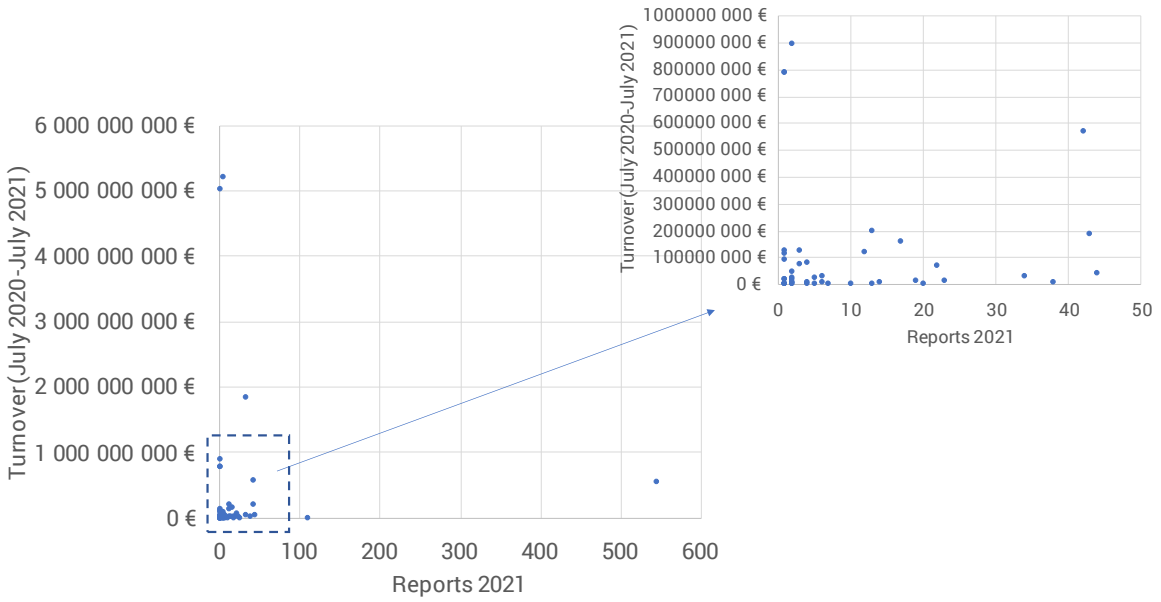


Figure 6. The number of reports sent in 2021 to the FIU by VASPs (1.01-5.10.2021) and the volume of turnover related to virtual asset services (in the period July 2020-July 2021).

The content analysis of the reports received and the executed supervision inspections among market participants indicate that the level of application of due diligence measures of the majority of market participants is insufficient and the majority of VASPs lack effective surveillance and monitoring systems that take into consideration the specifics of the field of activity that would allow the timeous identification of transactions suspected of money laundering or terrorism financing. During the first nine months of 2021, VASPs mostly sent reports about the suspicion of the presentation of forged documents in the phase of establishing a client relationship. There were many notifiers whose reports solely or predominantly contained the suspicion of using a stolen identity or information received from an external party (e.g. a client with a criminal background; a fraud case that the VASP is informed about by the fraud victim or his/her bank). This is a stark warning about the market as a whole: it can be concluded that these service providers do not sufficiently monitor the remaining client relationship or transactions. This suspicion is further deepened by the circumstances that a part of the VASPs lack blockchain analytical tools with the capacity to identify dark web or mixer transactions. It's not believable that service providers that have a turnover in the tens or hundreds of millions of euro do not have a single suspicious transaction or client e.g. about the legal origin of the property or the legality of the transaction.

Content analysis of reports also shows that only a few isolated service providers' due diligence systems are sufficiently developed (allowing for the identification of dark web and mixer transactions; transactions related to each other that when viewed as a whole arouse suspicion) and only a few apply due diligence measures with a surveillance system that has been developed by the company itself (e.g. a large transaction, numerous small transactions related to one another, the total of which is large, other changes in the activities of the client compared to its original profile etc.). It can be stated, based on the content analysis of reports, that the majority do not sufficiently apply "know your client" or due diligence

measures that allow the identification of legal origin; their systems are not sufficient to minimise the risk that through them, terrorism is financed or sanction regimes are violated.

2.4. THE RESULTS OF THE SUPERVISION PROCEEDINGS, OF THE FINANCIAL INTELLIGENCE UNIT

The supervisory department of the FIU has supervised VASPs since 2018. The FIU before that executed supervision over providers of alternative payment institution service, among whom in terms of the content of service, also belonged to companies offering services equivalent to VASPs. The FIU in the case of all supervision inspections detected deficiencies in the activities of the company.

Table 5. Supervision inspections on VASPs and measures taken as a result of supervision inspections, during the period 2018-2020

Action	2018	2019	2020	2021
Number of onsite supervision inspections	26	34	13	14
Number of remote inspections	23	29	864	606
Number of licenses for the provision of virtual asset service that have been declared void	29	97	1784	329
Number of licenses declared as void as a result of supervision inspections	20	31	8	1
Number of precepts issued for liquidating deficiencies, as a result of supervision inspections	1	3	0	0
Number of compensation levies applied	3	11	3	1
Number of misdemeanour proceedings	1	4	1	0

It has, as stated above, proven to be difficult over the years to execute supervision over the field. The FIU has noticed through daily activities that the VASPs do not respond to the precepts (information requests) of the FIU, wherefore the FIU cannot obtain information for investigating money laundering and terrorism financing, as well as executing supervision. There are many reasons for not responding, incl. that the e-mail addresses presented to the FIU, are invalid or the subject simply lacks the corresponding information. It has been difficult or impossible in many cases, as companies are not located at the addresses, presented as their place of activity to the FIU, to contact the representatives of the company. This is also one of the reasons why licenses of many companies, have as a result of supervision been declared void. The reason for declaring as void has been the repeated not responding to the precept of the supervision department, where to the supervision institution is not presented the demanded data and information on the activities of the company.

There have been numerous deficiencies in the rules of procedure and risk assessments, in those companies where it's been possible to execute supervisory inspections, due diligence measures have not been applied correctly, identified politically exposed persons, beneficial owners etc. The FIU, resulting from this has initiated misdemeanour proceedings and compiled precepts for liquidating deficiencies.