13. Additional risk analysis of the riskiest sector of the National Risk Assessment, i.e., the sector of virtual currency service providers, based on the developments in the period 2020-2021

This chapter of the Report was prepared by the working group including the representatives from the following authorities:

- Financial Supervision Authority
- Internal Security Service
- National Criminal Police
- Tax and Customs Board
- Financial Intelligence Unit
- Prosecutor's Office
- Ministry of Finance
- Ministry of the Interior

13.1. Risks related to virtual currency service providers (incl. activity licenses)

13.1.1. Virtual currency service providers (hereinafter: VC) sector statistics from supervisory and law enforcement agencies

Table 113. Statistics of the Financial Intelligence Unit (FIU) on VC licenses in 2020-2021

Year	**2020**	As at **10 Mar 2021**
Applications for VC licenses	633 new requests (in addition 601 change requests). 368 licenses were issued	71 new requests (plus 69 change requests) 61 licenses were issued
Valid licenses	383 (as at 31 Dec 2020)	444
Relationship of VC service providers with non-residents	129	3
Suspicious transaction notifications related to VC service providers	108	10
Foreign inquiries regarding VC service providers licensed by FIU	42	18
Supervisory procedures carried out	13	1

In 2020, the FIU managed to carry out inspections of 13 VC service providers.
The PBGB received the following inquiries about persons holding a VC license in 2020:

- A total of about 50 foreign inquiries on 23 different legal entities, relating to scams, money laundering, and cybercrime. Of these, 19 legal entities are related to non-residents.
- 30 requests for judicial assistance concerning 4 different legal entities, where the majority are related to the investment fraud. In the requests for judicial assistance, the damage caused has been estimated to a total of more than 1 million euros. All of these legal entities are affiliated with non-residents.

Regarding VCs, different information is constantly received by supervisory and law enforcement authorities:

- According to the information received by the PBGB, VC licenses are handled by the company service providers on whom different information has been received in connection with economic crime.
- The information received by the Financial Supervision Authority on virtual currency service providers concerns possible fraud-related cases, where fraudulent benefits have been transferred to VC service providers licensed in Estonia.
- The Internal Security Service has identified the use of virtual currencies to support terrorism.

In conclusion

The demand for and interest in VC activity licenses have not decreased, on the contrary, they are on a growth trend again, despite the additional requirements that came into force in the summer of 2020 for applying for licenses. At the same time, the number of foreign inquiries has not decreased, which suggests that despite the tightening of the rules, suspicious transactions attracting the attention of foreign law enforcement authorities continue. From the above, two conclusions can be drawn:

1. Suspected fraudulent activities of companies with VC licenses are becoming more active.
2. Despite the stricter requirements, application for VC licenses is becoming more active, which, taking into account the growing large number of subjects of supervision and limited supervisory resources, is complicating taking this field under the state's control.

13.1.2. Risks in the VC service providers sector

Based on the analysis of the above statistics, information, and experience of the members of the working group, the following risks related to VC service providers have been identified:

- **At the general national level:**

  (a) **Low level of regulation, supervision, and transparency.** The risk to the society is mainly due to the fact that the service is not sufficiently regulated and the supervisory resource is disproportionate to the number of subjects operating in the sector, which weakens timely and risk-based supervision, while the service itself poses real money laundering and terrorist financing risks. This, in turn, reflects **a very low level of transparency in the sector and a lack of complete risk mapping**. Estonia is specifically characterised by **an exceptionally large number of subjects in the sector** who have an activity license issued in Estonia but whose economic activities are directed outside Estonia, which is why connection with the Estonian economy is very weak or non-existent. The Estonian state issues activity licenses for virtual currencies without sufficient capacity to subsequently verify compliance with the requirements of the activity license and operational requirements (incl. due diligence obligations in relation to money laundering and terrorist financing). As a state, we take responsibility by "guaranteeing" the reliability of the licensed companies while having no **actual opportunity to prevent or mitigate the risks involved.**

  b) **Extensive damage to reputation.** Virtual currency service providers, in general, are at the same time the subjects of many typologies, carrying the risks of money laundering, terrorist financing, and weapons of mass destruction proliferation financing. In combination with the aforementioned risks and the multiplicity of the subjects**, Estonia is currently exposing itself to exceptionally high levels of financial crime and thus to a large risk of reputational damage.** The Council of Europe's expert committee MONEYVAL also critically evaluates this issue, which is why Estonia's activities in relation to virtual currency service providers have an extremely significant **negative impact on many criteria**, bringing Estonia significantly closer to the process of recognising Estonia as an internationally risky jurisdiction.

  c) **The VC service involves a high security risk.** Data already obtained from individual companies indicate a serious security threat that can only be mitigated through the application of enhanced measures that include a set of deterrence measures, including mitigation of the market participant business risk appetite (more detailed proposals are described in the table).

  d) **An increased risk due to e-Residency.** The field of virtual currencies, combined with the possibilities of taking advantage of Estonian e-Residency, creates a **multi-layered scheme**

enabling anonymity, with great potential for terrorist financing, and due to the structure of the sector, this theoretical risk cannot be eliminated by any hedging mechanisms other than changing regulations and supervision to a significant extent. According to statistics, there have been 411 e-residents in the case of invalid licenses (incl. 6 from Turkey, 2 from Bangladesh, 2 from Lebanon, 2 from Jordan, 2 from Tunisia, etc.), a total of 38 e-residents are involved in valid licenses (out of risk countries, only Russia with 6 licenses). It is important to draw attention to Russia's connection, as it includes the Caucasus region, which is home to a significant number of Islamic extremist fighters staying in or returning from conflict hotspots.

e) **No actual connection to the state.** Foreign countries ask for information (mostly in cases of scams), where the money has been transferred to an Estonian account belonging to a payment intermediary registered in a foreign country and located in the jurisdiction of that country. The Bank of Estonia (Eesti Pank) does not see the customer information of this payment intermediary, especially if it is a VIBAN account and the other country does not know that it is a payment intermediary, e.g. from the UK. Today, it is possible to communicate directly with a payment intermediary, but the fact that an **Estonian bank account number is used is still misleading to other countries**. Estonia is not able to respond to foreign inquiries, which damages the trust of our partners and is misleading as to our willingness to cooperate. Due to the weakness of the connection, the possible positive contribution to the Estonian economy, including the generation of tax revenues or business revenues, is marginal.

(f) **Difficulties in the application of due diligence measures due to Covid-19.** The Covid-19 pandemic is cited as an excuse why **it is not possible to fulfil the circumstances of the controlled object in time when applying for licenses, or why, for example, the contact person cannot come to an interview**, etc. One risk point, however, might be (though hypothetical at the moment, since the supervisory authorities have not been able to carry out a lot of on-site inspections in terms of VC after the law amendment) that as many of VC providers are foreigners, they are more likely to stay in their home country, due to which it **is not possible to carry out supervision on-site**. For example, in a misdemeanour proceeding of a virtual currency service provider, the current situation is that the member of the management board (the person subject to proceedings) is in the UK and cannot be questioned.

- **At the supervision-specific level:**

  a) Issues related to the location of the management board: § 72 (1) 4) of the Money Laundering and Terrorist Financing Prevention Act stipulates as an object of inspection the location of the management board which must be in Estonia. The law stipulates and the explanatory memorandum shows that the location is determined by the importance of the duties of the member of the management board, i.e., the management board is located where substantive management takes place: important management decisions are made and the members of the management board performing support tasks may also be located abroad. In practice, it is difficult to determine how the areas of work and responsibilities of the members of the management board are actually divided, because we can only rely on the explanations and documents that the members of the management board may produce by distorting reality. In conclusion, there is a high risk that, for example, if a company has two members of the management board, the member of the management board located in Estonia is a figurehead for whom evidence has been submitted as a responsible member of the management board. According to the information received by the PBGB, Estonian persons who are not actually involved in the company's operation have been registered as members of management boards.

  b) The representative of the management board as a figurehead. One and the same person is a member of the management board in several companies, i.e., more companies are emerging, but it is not clear why one person needs so many of them, and another problem is that **the member of the management board is therefore a figurehead**. Based on the current practice, an activity pattern emerges **where company service providers and law firms submit proper documentation when applying for an activity license and then the people**

on the management board withdraw from the company's management, often a change takes place also in the management body, where a random **board member is introduced who does not have real access to data.**

c) Contact person as a figurehead. The contact person has been declared as a contact person in several companies, so it is not possible to ensure confidentiality in communication with supervisory and law enforcement authorities. There have also been cases where the **contact person is a figurehead who does not know anything about the company's operation**. When an inspection is performed, that person must always ask someone else for information, to which he or she should have direct access due to his/her job.

d) A rapid increase in the number of VC service providers, insufficient resources for supervision, and short inspection time. Although at first sight it may seem that these problems can be detected, prosecuted, and sanctioned through supervision, this is essentially impossible due to the mass of infringements. The number of VC service providers is on a growth trend again in 2021, e.g., 71 new applications were submitted to the FIU in the first three months, in addition, 69 change applications have to be processed. In 2020, the FIU issued 368 activity licenses. At the time of preparing this compilation, a total of 444 companies had the license of a VC service provider. **It is not possible to check the content** of all the documents that must be submitted when submitting an application for an activity license (for example, the rules of procedure and internal control rules specified in § 70 (3) 5) in terms of whether they correspond to the actual service provided, there are no resources and a time is limited to process the applications (60 days, which may be extended to 120 days). A lack of resources, a high workload, and the deadlines create a situation where the performance of **substantive supervision is vulnerable and low. In Estonia, it is not possible to recruit sufficiently competent supervisory officials within a reasonable period of time, even if a resource is allocated to the supervisory authority for this purpose. The multiplicity of negative decisions, in turn, increases the number of litigations and the workload of courts. The weak connection with Estonia complicates both supervision and court proceedings under Estonian law.**

e) Restrictions on transactions. Restricting virtual currency transactions is problematic, as it **is not always proportionate to limit the (payment) intermediary's account because he or she is not the owner of the property**. **Criminal assets do not stand in the wallet of the VC for a long time, but quickly move along.**

- **At the sector-specific level:**

  a) Insufficient application of due diligence measures by VC providers. Although the FIU has carried out supervisory procedures at a small number of companies, their inspections revealed that the deficiencies were mostly related to the application of due diligence measures and data recording. The KYC (Know Your Customer) requirements are applied at **very different qualities**.

  b) The contact person of the VC company AML does not have substantive access to the transaction information and has no knowledge. The service of a law firm which has helped to apply for a license, but which has no connection with day-to-day activities is often used. **The AML contact person is a minimum-paid figurehead who lacks knowledge and real access to the data.**

  c) Anonymity of VC transactions. Until **it is possible to link a specific wallet number to a specific person**, the block chain is largely anonymous. Software for tracking block chain transaction is there for only more common VCs.

  (d) Low level of notifications. In the view of pre-analysis and analysis of information, the problem is the low **fulfilment of the notification obligation**. Only 1% of virtual currency companies have **complied with the notification obligation provided for by the Money Laundering and Terrorist Financing Prevention Act** (only 5-7). The notifications mostly concern anomalies identified during the establishment of the customer relationship. Suspicious transactions are rarely notified, i.e., the FIU does not receive important substantial information. This is certainly also due to the fact that **VC service providers are not able to identify persons related to external wallets. Therefore, they also lack clarity on what the**

client's field of activity is, nor do they understand what the client is doing. In order to prevent terrorist financing, the Internal Security Service has, based on a random sample, requested from some companies the customer lists from the areas of high risk of terrorism. **At least 2 foreign fighters returning from Syria have been identified in one company alone, in the other case more than 1,700 customers from high-risk countries** (incl. 272 from the Palestinian Authority, 67 from Yemen, 26 from Syria, etc.), in the third case (Estonian company without a FIU license) 210,665 "high-risk country" customers (including 70,796 from Yemen, 25,598 from the Palestinian Authority, 1,689 from Syria, 1,491 from Iraq, etc.).

e) **VC service providers do not have the necessary data on the customer**. The data obtained from the above inquiries indicate a serious quality problem: personal data is incorrect, the contact details provided are incomplete and unverified, a driving license is used as an identity document (if one is asked for), and identity checks are usually made using software of varying quality. Attempts to establish a customer relationship through a false identity are clearly outlined on the basis of these few reports of suspected terrorist financing by VC companies with a lack of due diligence, in most cases, providing additional information is refused and a refund of the initial payment is required. It is worth noting the transactions of Iranian citizens with Iran's own FinTech companies (so-called Exir.io, ExCoino, etc.), which **may indicate attempts to circumvent international sanctions.**

Summary

Considering:

1. The inability and/or unwillingness of VC service providers to perform the required due diligence obligations, including the obligation to know their customer;
2. The inability of state supervision to respond in an operative manner to the non-fulfilment of the aforementioned due diligence obligations arising from a large number of VC service providers and the transfer of activities outside Estonia;
3. The general lack of transparency of the field of activity of VC service providers (incl. their cross-border digital nature) due to the nature of the field and under-regulation caused by the novelty of the field;

the risk of money laundering and terrorist financing and the financing of the proliferation of weapons of mass destruction arising from the field of VC service providers must be assessed as high.

13.2. Proposals for risk mitigation measures in the virtual currency service providers' sector

When selecting the measures to be taken to mitigate the identified risks, the adequacy of the supervisory tools provided to the supervisory authority and the resources allocated to supervision, as well as the possibility to start from scratch with issuing licenses, must first be considered. As the risks at the national level are significantly high, exceptional measures, i.e., the suspension of the issue of licenses, should also be considered.

In assessing the applicable law and taking into account the specific nature of the risks in the VC service providers sector, the following options should be considered as countermeasures against the risks of money laundering and terrorist financing:

1. In order to prevent further escalation, apply the possibilities for background checks arising from the law when issuing activity licenses, and require, on the basis of § 70 (3) 5) of the Money Laundering and Terrorist Financing Prevention Act and relying on § 14 (1) and § 13 (4) of the Money Laundering and Terrorist Financing Prevention Act, that the rules of procedure and internal control rules, presented while applying for an activity license, effectively mitigate and manage, inter alia, the risks identified in this risk assessment.

2. To establish with the National Risk Assessment:

(a) The sector of VC service providers as a sector which is required to apply enhanced measures of due diligence:

(b) to complement the enhanced due diligence obligations imposed on the VC service providers sector by following:

- Enforcement of the "Travel rule"[1]. With this the same rules will be extended to VCs as these are set for the information on the payer and the recipient of the payment to be collected and transmitted in the case of money transfers,
- All persons who have established a customer relationship and/or use the platform for the transaction must be identified.
- The customer can only be identified on the basis of an identity document accompanied by a so-called profile photo.
- To make the KYC automated solution systems more effective.
- For "risk countries" clients, require person's involvement in the identification process.
- The identification must be accompanied by a valid mobile phone number and an e-mail address, the validity of which is checked semi-annually (sending verification codes).
- If several wallets are owned by the same person, they must be linked.
- PEP status checks must be guaranteed when establishing a customer relationship, requesting the customer's first payment to be made through the bank account of an EEA credit institution.
- Control and enforcement of international sanctions.

(c) to give the following guidelines to the authorities involved in the supervision of VC service providers:

- to prioritise the supervision of the VC service providers sector;
- to analyse the adequacy of the supervisory measures to ensure the supervision of the implementation of enhanced due diligence measures by VC service providers and, if necessary, to submit relevant proposals for amending the law;
- to assess the additional resources needed to increase the supervisory capacity of VC service providers and propose the allocation of funds;
- to take steps to raise awareness of the anti-money laundering and anti-terrorist financing in the VC service sector.

3. At the legislative level, to make the following changes:

a) to establish by a regulation of the Minister of Finance on the basis of the proposal of the FIU, a regular reporting obligation for the sector of VC service providers;

b) to review of the Money Laundering and Terrorist Financing Prevention Act and other legislation:

- To review and extend the grounds for the revocation of the license. The grounds for revocation should be mirrored in full compliance with the conditions for market entry and operation; each condition for entry and operation must be met by the possibility to address the circumstances through the license authorisation procedure. For the issuer of an activity license, the range of provisions provided for by law must be expanded, on the basis of which the issue of an activity license can be refused, including taking into account intelligence information of law enforcement agencies, international communication, and, if necessary, a memorandum from security authorities.
- To set restrictions on applying for a new activity license. Companies that have lost their license or received a negative decision and members of the management board should be subject to stricter rules for returning to the market.

[1] FATF Recommendation 16.

- To establish a ban on transferring the ownership after applying for an activity license. Within the next six months from the moment of applying for an activity license, the transfer of ownership of an enterprise with an activity license is prohibited.
- To set a higher barrier to market entry: appropriate requirements for assessing the suitability of managers/owners and the origin of capital, background checks; avoiding "forum shopping" – a significant increase of the activity license processing fee, a connection of the activity with Estonia[2]; requiring as a precondition the supervisory cooperation with the relevant jurisdictions (owners, countries of destination of the service)[3].
- To set higher requirements for the position of a member of the management board (comparable to, for example, the requirements of a contact person): When changing Fit & Proper requirements, to consider what could be taken over and what not from the Credit Institutions Act, to also consider consumer protection and market suitability requirements; there is some degree of market suitability within the supervision of Money Laundering and Terrorist Financing Prevention Act, but this is from the notion of money laundering and terrorist financing, not from the company's ability point of view to provide services to customers on the market).
- To complete the list of requirements for the contact person: Additional requirements for the position of a contact person, including a restriction in how many companies one contact person may work.
- To complete the list of requirements for the AML representative of the VC service provider: An AML employee with the necessary knowledge, with a physical location in Estonia who has real access to transaction information. Knowledge and physical location are checked before a license is issued. Periodic reporting requirement. Law firms in the activities of AML representatives must be excluded; there must be an official employee of the company for this purpose.
- To impose additional requirements for the location of operation: Imposing additional substantive requirements for the location of operation. Physical access to data must also be guaranteed in Estonia. The requirement to keep copies of documents, profile photos, and contact numbers of persons who have established a customer relationship.

4. Other necessary measures:

- Not to allow anonymous virtual currencies on platforms with an Estonian license.
- To consider establishing a national central VC register without transaction data. The register would contain: the name of the service provider, the client's first and last name, date of birth, country of birth, residence, citizenship, mobile phone number, e-mail address. Such data could slightly mitigate the risks. There is no other way to reach 400+ market participants and expecting them to apply due diligence would be an illusion.
- To introduce an asset and payment-based annual supervisory fee for the VC service sector.

[2] Similarly to clause § 19 (1) 7) of the Payment Institutions and Electronic Money Institutions Act.
[3] The existence of a supervisory MoU or other appropriate recognised framework for cooperation to the same standard.