7. Vulnerability of the FinTech sector

7.1. General description of the sector

Description of the sector:

Estonia is one of the most developed digital societies[1] and Estonians are considered tech-savvy – this statement is supported by the respective OECD study[2]. Digitalisation enables efficiency, greater competition and innovative services. At the same time, relying on digital infrastructure with complex value chains and various service provides, fast innovation and growing pressure to reduce costs produces new vulnerabilities and risks.

This national risk assessment (NRA) concerning the Estonian financial technology (FinTech) sector analysed the threats related to the provision of virtual currency services (virtual currency wallet service and virtual currency exchange service) and crowdfunding services. The NRA methodology for the FinTech sector prescribed only the assessment of risks related to virtual currencies, but with the approval of the FinTech working group, crowdfunding services were also included in the assessment.

FinTech sector working group sees a distinct need to analyse the subsectors of the Estonian FinTech sector in more detail in the next the risk assessment. In the future, it is necessary to assess other crypto assets aside from virtual currencies, both by separate token types and in terms of services related to crypto assets. There are multiple service providers on the market who are not under financial supervision but who provide various FinTech or related services to the subjects of financial supervision. Threats related to said entrepreneurs should also be analysed in the future because there is currently no overview of the related threat vectors. In terms of future risk assessment, the methodology used for assessing the referred entrepreneurs should also be considered.

Table 34. FinTech sector description.

Market participants	Number of market participants[3] as at 31.12.2019	Number of market participants as at 31.12.2020	Number of obliged entities	Presence of professional association or umbrella organisation
Virtual currency service providers[4]	1201[5]	419[6]	100%	Estonian Cryptocurrency Association
Crowdfunding service providers	N/A	34[7]	17.6%	No general umbrella organisation but some service providers are members of NPO FinanceEstonia.

[1] TalTech, FinTech Report Estonia 2019, p 13, https://old.taltech.ee/public/m/majandusanaluusi-ja-rahanduse-instituut/FinTech_Report_Estonia_2019_final.pdf.

[2] Measuring the Digital Transformation, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

[3] In case of virtual currencies, persons who have submitted a notice on temporary halt in economic activities have also been considered.

[4] Data from the register of economic activities, https://mtr.mkm.ee/.

[5] Including 1188 service providers that exchange a virtual currency against a fiat currency or a fiat currency against a virtual currency, and 1083 virtual currency wallet service providers, among whom are many concurrencies.

[6] Number obtained by adding up 383+36; i.e. 383 virtual currency service providers, 31 providers of a service of exchanging a virtual currency against a fiat currency and 29 virtual currency wallet service providers (latter two consist of 36 companies in total).

[7] An estimated number. The list of service providers is compiled based on information obtained from public resources.

Survey conducted within the NRA took place during the period when a large number of companies that previously were granted authorisation to provide services related to virtual currencies had their activity licenses revoked. Therefore, the feedback regarding virtual currencies is considerably more modest than initially presumed. Crowdfunding subsector activity was high.

Table 35. Data from the survey conducted in the FinTech sector.

Subsector	Number of market participants	Sample volume	Sample size/number of required responses	Number of invitations sent	Number of received responses	Response rate
Virtual currency service providers	951	sample	274	951	14	47%
Crowdfunding service providers	34	sample	30	34	100	36%

Virtual currencies

Crypto-assets is a term that is not defined in the Estonian law but conditionally all instruments that are presented in a cryptographic format could be considered crypto assets. Crypto-assets can be divided into three categories based on their main function and purpose. These are payment tokens or virtual currencies, investment tokens and utility tokens.[8]

There are more than 9,000 virtual currencies in the world.[9] Most virtual currencies use blockchain technology. Blockchain that is the basis of the virtual currency is a shared digital database that stores the transactions and that cannot be altered, making the data forge-proof and permanent. Transaction details are public and observable throughout[10],[11] but not the details concerning persons.

Centralised and decentralised virtual currencies are differentiated. Centralised virtual currencies have a central administrator who issues the virtual currencies, administers their use, and removes them from circulation. These can often be found in web environments that offer alternative payment networks or online games. Decentralised virtual currencies, e.g. bitcoin, do not have such central administrator.[12]

More narrowly, currencies could also be differentiated from cryptocurrencies. This is a money system constructed on cryptographic bases that are usually decentralised and self-regulating. Cryptocurrency is quite transparent for the user as the transactions are publicly observable, but the system allows anonymity. Cryptocurrencies include the majority of the well-known virtual currencies such as bitcoin, ethereum[13].[14]

Virtual currencies also include the so-called stablecoins, the price of which is linked to the value of some specific asset, most commonly 1:1 with the US dollar (some examples include Tether, USD Coin, Paxos). A stablecoin Libra is also currently being developed, which will connect and combine stablecoins (USD, EUR, GBP) and will be as a digital composite of them. Although essentially, the stablecoins do not bring about any higher risks than the virtual currencies in general, their potential for

[8] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 10.
[9] As at April 2021 according to web portal CoinMarketCap. Available at https://coinmarketcap.com.
[10] Journal *Ärileht*. *Plokiahela tehnoloogia* (Blockchain technology). 14.01.2019
[11] Estonian Financial Intelligence Unit, virtual currency service providers survey, p 3, 22.09.2020. Available at https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[12] Keatinge, T., Carlisle, D., Keen, F. (2018). Virtual currencies and terrorist financing: assessing the risks and evaluating responses. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. Estonian Financial Intelligence Unit, virtual currency service providers survey, p 3.
[13] See https://www.kryptoraha.ee/tehnoloogia/.
[14] Estonian Financial Intelligence Unit, virtual currency service providers survey, p 3, 22.09.2020. Available at https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.

mass use, the consequences of which are difficult to precisely assess at this time, are somewhat alarming[15].[16]

Virtual currency is defined in Estonian law as a value represented in digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds /.../ or a payment transaction /.../ (clause 3 9) of the Money Laundering and Terrorist Financing Prevention Act (hereinafter MLTFPA). Virtual currency service in turn is divided into virtual currency wallet service and virtual currency exchange service (see more details below from the information on the legal framework of the sector).[17]

The latest overview on the Estonian virtual currency service providers is available from the public survey published by the Estonian Financial Intelligence Unit (FIU) on 22.09.2020.[18]

The total turnover of virtual currency service providers active on the Estonian market has increased rapidly. While in 2018 said turnover was approximately 590 million euros, then by the first half of 2019 it had doubled to 1.2 billion euros.[19] The turnover of virtual currency service brokerage vary greatly between companies. During both periods, the highest turnover of one company reached 420 million euros in 2018 and 820 million euros in the first half of 2019. Among the companies that had started providing the service, the median turnover of mediated services was 94,000 euros in 2018 and 50,000 euros in the first half of 2019. 83 or nearly a third of the virtual currency service providers had intermediated services in 2018 and 188 companies were dealing with that in the first half of 2019.[20]

Virtual currency sector characteristics

Virtual currency is a digital value that is transferable, preservable or tradable, which is not the legal tender of any country or funds, but which natural persons or legal persons accept as a payment instrument (see AMLD V and MLTFPA[21]).[22] In Estonia, virtual currencies are deemed assets in the meaning of subsection 15 (1) of the Income Tax Act (ITA) and the income derived from these assets (income from transfer of property, salary income, business income from mining) is taxed based on the same principles as income received in traditional currency[23].[24] Transactions are digital and do not necessarily need a third person for execution, making their movement faster than regular financial transactions. For this purpose, revoking such transactions is difficult, if necessary.

[15] FATF. (2020). Virtual Assets – Draft FATF Report to G20 on so-called Stablecoins.

[16] Estonian Financial Intelligence Unit, virtual currency service providers survey, p 3, 22.09.2020. Available at https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.

[17] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 11.

[18] Virtual currency service providers survey, available at: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.

[19] The data is based on the FIU's virtual currency service providers survey and are estimated, as all subjects did not respond to the referred survey and the calculations are made based on the received responses.

[20] Sourcehttps://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b. Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 17.

[21] Clause 3 9) of the MLTFPA: Virtual currency' means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive;

[22] Estonian Financial Intelligence Unit, virtual currency service providers survey, p 4.

[23] Source: https://www.emta.ee/et/eraklient/tulu-deklareerimine/muu-tulu/eraisiku-virtuaalses-valuutaskruptovaluutassaadud-tulu.

[24] Estonian Financial Intelligence Unit, virtual currency service providers survey, p 4.

Crowdfunding

Crowdfunding is a method of financing that allows raising funds for projects and companies from many people using a specially designed environment (e.g. a crowdfunding platform).[25] Crowdfunding is an increasingly popular form of enterprise that on the one hand is beneficial for small and medium sized companies as it allows using the crowdfunding platform to raise capital, and on the other hand, retail investors can earn income with smaller investments as well. Crowdfunding offers alternatives to traditional financial services and helps to strengthen competition on the financial services market. The task of crowdfunding service providers is to find the projects and supporters for the projects, i.e. the investors, and to offer a technical solution to bring the interests of the financing applicants and investors together, which has been facilitated also by the development of technology.[26]

In general, crowdfunding can be divided into peer-to-peer lending, equity crowdfunding and rewards-based crowdfunding.[27] European Commission divides crowdfunding into five main categories, and depending on the entrepreneur's business model the platforms may include hybrid forms that are made up from several categories:

1. ***equity crowdfunding*** – companies issue equity (also known as crowd-investing or investment crowdfunding) or debt instruments to the investors via the platform;
2. ***peer-to-peer lending*** – companies or physical persons apply for loans from the public using the platforms;
3. ***invoice settlement using crowdfunding*** – form of asset-based financing where companies sell unpaid invoices or claims separately or in bulk to investors using the platform;
4. ***rewards-based crowdfunding*** – persons donate to a project or a company and later receive non-monetary fee for their contribution (e.g. goods or services);
5. ***donation-based crowdfunding*** – persons donate funds for additional financing of a specific charity project while not gaining any monetary or material income themselves.[28]

Table 36. Crowdfunding volumes in Estonia (m EUR)[29]

Year	2014	2015	2016	2017	2018	2019	2020*
Volume of mediated funding	29	41	66	95	168	313	196
Funding balance at the end of period	29	50	93	144	235	370	414

Crowdfunding sector characteristics

Crowdfunding sector stands out from other service providers in the financial sector because at this time, the crowdfunding service providers are not required to have an authorisation or registration to provide crowdfunding services. Therefore, there is no detailed overview of the actual number of crowdfunding service providers in Estonia and thus it is impossible to assess specific volumes.[30] The number of crowdfunding service providers interviewed within the FinTech sector is 34, the majority of whom (82.4%) are not obliged entities in the sense of the MLTFPA. Among the crowdfunding service providers there are 6 obliged entities in the meaning of MLTFPA. Described crowdfunding service providers are either subject to financial supervision and they require authorisation to operate (creditor or credit

[25] European Commission. Crowdfunding explained. 29.09.2015, p. 6. Available online at: https://ec.europa.eu/growth/content/crowdfunding-explained-0_en.
[26] Eesti Pank, Overview of finance sector, 2019, p 20.
[27] Source: https://ec.europa.eu/growth/tools-databases/crowdfunding-guide/types_en, https://www.fi.ee/et/finantsinspektsioon/finantsinnovatsioon/uhisrahastus.
[28] SNRA 2017 and 2019. NRA FinTech sector document analysis. See also Estonian FinTech sector vulnerabilities, document analysis, p 26.
[29] Source: Eesti Pank, public data sources; Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 15.
[30] Estonian FinTech sector vulnerabilities, document analysis, p 5.

intermediary (4); investment firm (1)), or they are a small fund manager without an activity license (1). Risks related with said persons are assessed under the financial services sector. Donation-based crowdfunding service providers are generally non-profit organisations (NPO-s) and threats related with NPO-s are also discussed in the NPO working group of the NRA.

FinTech sector legal framework

On 15 January 2021, the draft legislation on crowdfunding and other investment instruments and virtual currencies was published (*ÜMIVS*, in the process of being approved by stakeholders)[31]. The aim of the referred draft legislation is to regulate new and innovative capital raising methods with the main aim of ensuring stronger protection for investors.[32] With the referred draft legislation, a proposal is made to enforce operational requirements and supervision for the following entities operating in Estonia:

- crowdfunding platforms;
- entrepreneurs offering crypto assets, incl. virtual currency service providers;
- other entrepreneurs who provide so-called alternative investment options but are not yet subject to supervision.[33]

Since the public consultation of the draft legislation takes place in the first half of 2021, the final wording of the adopted act is currently not known.

Based on the aforementioned, the legal framework analysed within this assessment is currently being amended and made more efficient.

Virtual currency sector legal framework

Estonia is one of the first countries in the world where the activities of virtual currency service providers were regulated. Since it was discovered that developments in the field of information technology allow new practices for money laundering that are not subject to regulations in force, alternative means of payment service providers were subjected to the MLTFPA regulations in 2008.[34]

From 27.11.2017, Financial Intelligence Unit issues authorisations for providing virtual currency services in Estonia.[35] According to clause 3 9) of the MLTFPA, virtual currency means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4 (25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.[36]

Virtual currency service according to the MLTFPA is virtual currency wallet service and virtual currency exchange service. In case of wallet service, encrypted keys are created for the clients or their keys are kept, which are used for keeping, storing and transferring virtual currencies. In turn, virtual currency

[31] Draft legislation is available in the draft legislation information system, https://eelnoud.valitsus.ee/main/mount/docList/f4deaf4f-7351-4384-b3ae-aaa9621bf050 (document no. 21-0050/01, file no. 21-0050). See also the related press release https://www.rahandusministeerium.ee/et/uudised/rahandusministeerium-asub-uhisrahastuse-ja-kruptovarade-valdkonda-reguleerima.

[32] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 1.

[33] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 1.

[34] Estonian Financial Intelligence Unit, virtual currency service providers survey, p 4, available at: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.

[35] Financial Intelligence Unit, economic activity license. Available at https://www.politsei.ee/et/juhend/majandustegevuse-luba.

[36] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 11.

exchange service is divided into two: exchanging virtual currency against fiat currency or vice versa, or exchanging one virtual currency against another virtual currency.[37]

With the MLTFPA and the State Fees Act amendment draft legislation, which was adopted on 11.12.2019, many significant changes were made to the MLTFPA.[38] Most of the amendments entered into force on 10 March 2020. With the amendment, the virtual currency exchange service providers and virtual currency wallet service providers were gathered under single term – virtual currency service providers. According to the amendment, authorisations can be granted only to virtual currency service providers whose registered location, location of management board and place of business is in Estonia, or to a foreign company that operates via a branch entered in the Estonian commercial register and whose place of business and manager are in Estonia. Additionally, proper business reputation requirement was enforced for the member of the management body, procurator, beneficial owner and owner. Additionally, the authorisation applicant must have a payment account in a credit institution, e-money institution or a payment institution that is established in Estonia or in a European Economic Area member state that provides cross-border services in Estonia or that has opened a branch in Estonia. Requirement was enforced that the share capital of the entrepreneur applying for authorisation must be at least 12,000 euros which has been contributed in full. State fee for reviewing the application for authorisation was raised from 345 euros to 3,300 euros. Authorisations issued before the amendments remained valid but the persons to whom the authorisations had been granted had to make sure their activity complied with the conditions for issuing the authorisation, otherwise the FIU has the right to revoke the authorisation. One prominent change to the MLTFPA was that the requirements applied to financing institutions were also applied to virtual currency service providers. Therefore, the virtual currency service providers had to update internal control rules, procedural rules and risk appetite documentation. After the amendments, the virtual currency service providers had to consider the instructions of European supervisory authorities on risk factors upon discovering circumstances characterising lower or higher risk and when choosing simplified or enhanced due diligence measures. Additionally, the obligation to appoint a FIU contact person was enforced and identification requirements, incl. remote identification, became stricter for virtual currency service providers, and higher maximum penalty rates were enforced for repeated violations.

Crowdfunding sector legal framework

Pursuant to the regulation in force, crowdfunding service providers are divided into regulated and unregulated service providers, whereas certain specific legal acts for financial services apply to the former (e.g. Creditors and Credit Intermediaries Act, Securities Market Act). Regulation applicable for a crowdfunding service provider thus depends at this time on the company's business model and financing project structure, among else the entrepreneur must assess whether its activities have traits that require an authorisation, an activity license or registering its activities with the Financial Supervision Authority.[39]

In case of peer-to-peer lending, two types of crowdfunding should be distinguished: crowdfunding aimed at legal persons (mostly companies) and at physical persons (consumers). If the crowdfunding service provider wants to intermediate credit to the consumer, both the loan contracts and the activities of the service provider as the intermediary of consumer credit must meet the consumer credit agreement provisions according to paragraph 2 subsection 2 of the Creditors and Credit Intermediaries Act. This means, among else, that said entrepreneur must apply for a credit intermediary activity license from the Financial Supervision Authority.[40] Pursuant to the aforementioned, the activities of crowdfunding

[37] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 11.

[38] Draft legislation is available: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/24832445-95e0-4ffc-adbe-ec44d87d5eb1/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ning%20riigil%C3%B5ivuseaduse%20muutmise%20seadus.

[39] Estonian FinTech sector vulnerabilities, document analysis, p 6.

[40] Source: Letter of explanation for draft legislation on Creditors and Credit Intermediaries Act, p 12. Letter of explanation for the draft legislation is available on the Riigikogu website: Creditors and Credit Intermediaries Act 795 SE,

service providers that intermediate consumer credit are included as activities of creditors and intermediaries when preparing the national risk assessment, which is why money laundering and terrorist financing risks related to them are assessed under the financial services sector. Currently, the situation is similar in case of investment-based crowdfunding because depending on the activity model of the investment firm or fund management company, an activity license may be required. Risks related to the service providers that have been granted the respective activity licenses have also been assessed within the financial services sector risk assessment.

In 2016, the Financial Supervision Authority submitted an initiation to regulate crowdfunding.[41] Under the lead of NPO FinanceEstonia the crowdfunding best practice[42] was developed the same year, the aim of which was to make the activities of crowdfunding service providers clear and transparent for the clients (applicants for funding and investors). 4 entrepreneurs received a commendation in 2019 for following the non-mandatory guidelines[43].

On 7.10.2020, the regulation (EU) 2020/1503 of the European Parliament and of the Council was adopted (hereinafter also referred to as EU crowdfunding regulation)[44] and directive (EU) 2020/1504 of the European Parliament and of the Council that amends the directive (EU) 2014/65 (or the MiFID II directive).[45] Said legal acts are enforced on 10.11.2021 and 10.05.2021, respectively.

On 15.01.2021, the draft legislation on crowdfunding and other investment instruments and virtual currencies which will considerably change the legal sphere of the domain of crowdfunding in the future was submitted for the first round of approval.[46] Among else, this draft legislation introduces provisions that implement regulation (EU) 2020/1503 as well as provisions that implement directive (EU) 2020/1504 regarding liability and supervision over the crowdfunding service providers in the scope of the referred EU legal acts.[47]

7.2. Description of risk typologies

Common risks in FinTech sector and the typologies of such risks

Risks related to state or geographical location

- **cross-border activities and global grasp** (incl. transactions in high-risk jurisdictions)[48]
- **complexity of identifying the source of funds** (funds move across state borders quickly)

Risks related to services, product features and transactions, and distribution channels

- **provision of internet-based service** (incl. transactions in dark web)
- **the use of cash and virtual currencies which allow anonymity**
- **transaction speed** (transactions are quick, among else cross-border, which makes determining the movement of illicit funds more difficult)
- **problems with monitoring systems** (service providers' monitoring systems are unable to identify cashflows of illegal origin with sufficient effectivity)

https://www.riigikogu.ee/tegevus/eelnoud/eelnou/950bdd45-ccf9-468c-b66e511edb1d6e3f/Krediidiandjate%20ja%20–vahendajate%20seadus. TMKo 2-17-11472 p 2, HMKo 2-18-104070 c 23.

[41] Available at https://www.fi.ee/sites/default/files/2016_09_Uhisrahastuse_seaduse_eelnou.pdf.

[42] Available at http://financeestonia.eu/wp-content/uploads/2017/07/hisrahastuse-Hea-Tava-.pdf.

[43] See http://www.financeestonia.eu/priority_niche/crowdfunding/.

[44] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32020R1503&from=EN.

[45] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32020L1504&qid=1606384145932&from=EN.

[46] See text on ÜMIVS draft legislation above.

[47] Letter of explanation for the draft legislation on crowdfunding and other investment instruments and virtual currencies, page 9-10.

[48] See also http://www.fatf-gafi.org/countries/#high-risk.

Risks related to clients

- **problems related to identification** (incl. transactions with high-risk clients; service provider cannot identify the transaction the other party of which is a politically exposed person (PEP), either due to the shortcomings of the screening system or lists of PEP-s)
- **complexity of determining the beneficial owner** (service provider cannot identify the beneficial owner due to the complicated ownership structure of the client or the other party, or due to the lacking information of beneficial owner in the register)
- clients who are **non-residents or are e-residents** (service provider is unable to implement respective due diligence measures for clients who are non-residents or e-residents because of complexity of determining their actual risk level)

Risks related to the regulative environment, incl. conducting supervision

- **under-regulation of the field** (rapid development of the field is one step ahead of the regulative environment, rapid development of technology allows the continuous launch of new services to the market)
- **global fragmentation of the relevant regulations** (different requirements, definitions, etc.)
- **cooperation with other countries' supervisory authorities may be problematic** (especially with the competent authorities of third countries)
- **cooperation between service providers and competent authorities** (service providers would like more cooperation with competent authorities and more efficient trainings)
- **shortage of domain-specific instructions and guides** (service providers are unable to identify transactions aimed at financing terrorism or the proliferation of WMD-s)

Criminal activity

- **fraud** (incl. fraudulent conduct, e.g. investment frauds; service provider is unable to identify a fictitious transaction (fictitious documents related to a transaction) or a person (fictitious identification documents))
- **cybercrime** (incl. internet fraud, virtual extortions, attacks on computer systems, compromising data (incl. information theft, manipulations), attacks on service provider's systems, infecting websites with viruses, crypto mining, attacks on mobile wallets)
- **transactions in the dark web**
- **offences related with narcotics**

According to literature[49], the general risks of FinTech increase with providing digital financial services and accompanying problems, e.g. identification. The use of electronic identification and reliability become even more important in the future.[50] Money laundering and terrorist financing risks concerning virtual currency and virtual assets are generally deemed high or very high.[51]

7.3. Threats

7.3.1. Money laundering threats

Common threats

In this NRA, the **threat level** of FinTech sector was assessed[52] as follows:

Table 37. FinTech sector threat levels

[49] See for example 2019 SNRA.
[50] COM SNRA 2017 (Cross-European TF/ML risk assessment conducted by European Commission).
[51] COM SNRA 2019 (Cross-European TF/ML risk assessment conducted by European Commission, amended and supplemented version).
[52] Assessments given by the NRA threats working group, which are based on the risk assessment performance method.

FinTech sector	Money laundering threat level on the sectoral level		Terrorist financing threat level on the sectoral level	
Virtual currencies	**3**	average	**5**	high
Crowdfunding	**2.45**	average/low	**2.3**	average/low

Possible threats related to virtual currencies

Threats related to state or geographical location

- The cross-border nature of transactions allows concluding transactions with high-risk clients or clients from high-risk jurisdictions who cannot be identified.
- It is easy to transfer virtual assets to different countries and there are no global uniform control and prevention measures. Criminals use virtual assets, incl. virtual currency systems to anonymously transfer funds or buy products.
- Decentralised nature of virtual currencies (internationality and cross-border activities) does not allow efficient supervision and asset confiscation.
- Complexity of international cooperation.
- Lack of national cooperation.

Analysis of materialisation of a possible threat in Estonia

Internationality is one of the greatest threats in the Estonian virtual currency sector. According to the FIU's virtual currency service providers' survey[53], a significant number of entrepreneurs who have been granted authorisation for the provision of virtual currency service in Estonia have engaged in business activities abroad and have no connection with Estonia.[54] Also data on the locations of the bank accounts of virtual currency service providers refers to the companies' low level of affiliation with Estonia. At the time of responding to the survey, nearly 40% of companies had a bank account in Lithuania, 25% in Great Britain and 10% in Estonia. Only nearly 0.15% of all the clients of virtual currency service providers that hold Estonian activity license are from Estonia.

The global scale of virtual currency makes conducting supervision and investigation by law enforcement authorities difficult. Transactions are concluded across borders and using multiple service providers located in different jurisdictions. Thus it is difficult to determine in which jurisdiction the transactions are concluded in and how to ensure the availability of the respective information.

According to the FIU survey, difficulty with international cooperation remains a threat in Estonia. Cooperation measures with certain jurisdictions are not in place which makes discovering the schemes and preventing crimes complicated because almost all cases have international extent.

Opportunity to use fast financial technology as an "intermediate stop" contributes to the possibilities of layering the funds that have criminal or unclear origin. Fast and cross-border cashflows from jurisdictions not participating in effective international cooperation give the criminals a chance to direct the funds into legal business.

Due to the great business environment and e-state possibilities of Estonia, it is simple and affordable also for non-residents or e-residents to establish companies in Estonia. The market also includes sellers of so-called shelf companies who found companies that are sold to non-residents or e-residents, also offering a mailbox service, thus creating a deceptive connection with Estonia. In case of non-residents and e-residents from third countries, complexity of conducting background checks is also an issue. For example, the National Audit Office identified in 2020, the Police and Border Guard Board (PBGB) has

[53] Available at https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[54] Amendments to the MLTFPA enforced in 2020 have improved the situation.

issued a digital e-resident ID to a foreigner who has a valid criminal punishment abroad.[55] Adhering to the aforementioned, the threat that comes from companies with non-resident and e-resident owners may be considered "low/average".

Adhering to the aforementioned and in conjunction with subsection 2 (5) and clause 31 (1) 2) of MLTFPA, i.e. the obligation of virtual currency service provider as the financing institution to identify and check the identity of the person either on site or by using info technological means, the threats related with state or geographical location can be considered "average/high".

Threats related to services, product features and transactions and distribution channels

- Blockchain technology does not allow effective monitoring of transactions and identification of suspicious transactions, which reduces the capability of law enforcement agencies to trace criminal income. The transactions are complicated in terms of IT.
- Pseudo-anonymity, opaqueness and speed of transactions, incl. without revealing the owner of the transaction.
- Blurring transactions, i.e. to complicate the link between crime and obtained asset, trying to give the impression that the funds are legally earned.
- Being offered on the internet and as cross-border services, they possess a greater risk (incl. dark web transactions, transactions concluded in virtual assets or cash).
- Virtual currency mixing services allow greater privacy (e.g. illegally obtained virtual currency is mixed with legally obtained currency that makes tracing the movement of the asset considerably more difficult, if not impossible), faster transactions, lower transaction fees and lesser price fluctuations.
- Virtual currencies can be purchased for cash or using money transferred by third persons which is why it is not possible to properly identify the origin of the funds.
- Virtual assets, incl. currencies allow to access funds anonymously, hide transaction history, hold private keys, and withdraw cash from ATMs.
- Decentralised service provision channels (incl. ATMs).
- Decentralised platforms which cannot intervene into client's transactions.
- Such virtual currency service providers, who do not store private keys on behalf of the clients but offer so-called tools that allow the client to store one's own private key and therefore the service provider may not have access to the wallet, are also a threat.

Analysis of realisation of a possible threat in Estonia

Although virtual currencies and the respective sector originate from 2008, in general it was previously welcomed by enthusiasts and so-called virtual currency extremists whose priorities are anonymity and privacy. Even though virtual currencies are becoming increasingly popular also among regular users, primarily as instruments of investment or speculation, a large number of users have adopted the soto say extremist attitude, stressing the importance of their privacy. Pursuant to this, it is common in the virtual currency sector (compared to other sectors discussed in this report) that regardless of the demand of the obliged entity, the client refuses to submit the respective information when due diligence measures are implemented, and this is primarily due to the fear that their privacy is breached, and the respective data is immediately sent to the Tax and Customs Board.

Anonymity and opaqueness of transactions also attract criminals who see the possibility of legalising their money through virtual currencies. There is less transparency in case of virtual currency wallet owners and although the conclusion of transactions is technically public, the persons behind them may and most often will remain anonymous. To hide the transactions blurring measures are used which do not allow to observe the movement of assets. When crypto asset becomes fiat money, the person concluding the payment is usually the intermediary, which is why it may not be visible who the actual owner of the asset is. It is difficult for the service providers to control the asset origin if the virtual currency intermediary service provider has not followed due diligence measures properly.

[55] Source: https://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/ItemId/1294/amid/557/language/et-EE/Default.aspx.

Opaqueness of transactions helps criminals to move financial currencies quickly and this primarily via unregulated financial sector service providers. Virtual currency services are also on their radar. Lack of control gives the chance to "launder" their funds of illicit origin. All this is also enabled by complicated ownership structures and transactions between related persons. In case of smaller service providers, such transactions may not receive the required attention, among else due to lack of competent human resources.

It is possible to obtain virtual currencies also for cash, which is in essence anonymous and thus there is a threat of taking advantage of the financial system. Proceeds of crime may also be withdrawn in cash to erase the link between the proceeds obtained from criminal activities and its user.

Since owning a settlement or payment account is an obligation for virtual currency service providers pursuant to law – paragraph 72 subsection 1 point 5 of MLTFPA, then using regulated payment service providers may mitigate the threats to some extent.

Adhering to the aforementioned the threats related to services, product features and transactions and distribution channels can be considered "average/high".

Threats related to clients

- **Problems related to identification** (incl. transactions with high-risk clients; service provider cannot identify the transaction the other party of which is a PEP, either due to the shortcomings of the screening system or lists of PEPs).
- **Complexity of determining the beneficial owner** (e.g. anonymity or pseudo-anonymity of transactions, where the identity of the beneficial owner[56] can be identified using certain technologies; service provider cannot identify the beneficial owner due to the complicated ownership structure of the client or the other party, or due to the lacking information of beneficial owner in the register).
- Clients who are **non-residents or e-residents** (service provider is unable to implement respective due diligence measures to clients who are non-residents or e-residents because of complexity of identifying their actual risk level).

Analysis of materialisation of a possible threat in Estonia

There are no known issues with the identification of Estonian clients. Since the sector is international, identification of clients globally may be problematic (e.g. efficiency or availability of identification technologies). By implementing suitable due diligence measures to clients it is possible to keep the FinTech sector clear of people who might take advantage of it. Otherwise the criminals may move funds via undercover agents or companies making identification of the beneficial owner difficult. Threats are also present online when establishing customer relationships, because larger misuse of identification documents is a problem here. Smaller financing institutions may have problems with sufficient identification of non-resident clients and thus financial funds, the owner or origin of which is unclear, may end up in the FinTech sector.

Problems with implementing the know-your-client (KYC) principle have also been identified in the sector. Namely, there is a wide misconception that implementing the KYC principle means only identifying the client as per paragraph 21 of the MLTFPA (primarily implementing the principle of two sources according to paragraph 21 (4) of the MLTFPA), not the money laundering and terrorist financing due diligence measures as a whole according to paragraph 20 of the MLTFPA. Thus, the obliged entity who in addition to identifying applies additional and enhanced due diligence measures, causes displeasure among the clients, the consequence of which is that information and documents are not submitted which makes implementing due diligence measures impossible.

[56] According to subsection 9 (1) of MLTFPA, the beneficial owner is a physical person who has the final dominant influence over a physical or legal person or in whose interests, for the benefit of whom or in whose name a transaction is made. Final dominant influence is due to the ownership type or via controlling another person in another manner.

Adhering to the aforementioned, the threat related to clients can be considered "average/high".

Threats related to regulative environment

- **Under-regulation of the virtual assets sector.**
- **Problems with confiscation of virtual assets.**
- **Different requirements, incl. regulations at different levels in the EU member states and globally.**
- Since virtual currencies and assets are very innovative and in constant change, **definitions included in regulations** are also threats because these might eliminate certain services/products from implementing the regulations.
- **Cooperation with other countries' supervisory authorities may be problematic** (especially with the competent authorities of third countries).
- **Cooperation between service providers and competent authorities** (service providers would like more cooperation with competent authorities and more efficient trainings).
- **Shortage of sector-specific instructions and guides** (service providers are unable to determine transactions aimed at financing terrorism or the proliferation of WMD-s).
- **Shortage of specialised judges and competent supervisory officials.**

Analysis of materialisation of a possible threat in Estonia

Under-regulation of the FinTech sector is one step ahead of the regulative environment allowing continuous launching of new services to the market that are outside of the existing legal framework.

According to the FIU survey, the problem is also with unclarity in legislation and internal regulations of the PBGB concerning seizure of virtual currencies. Currently, it is simply resolved by agreement wherein the persons involved in the procedure are offered the option to put the currencies on the PBGB's crypto currency account or convert them into euros. It needs to be analysed whether the value of virtual currency in euros (not in crypto currency) provided in the court decisions is appropriate, considering the significant volatility of said currencies. The judges might also need additional knowledge (e.g. respective training) in certain matters concerning virtual assets.

In addition to cross-border nature and the user's option to choose a virtual currency service from any available service provider, the sector risk is also increased by lack of common provisions and legal arbitral tribunal. Agreeing on common norms and definitions across the EU is difficult (there is still no respective regulative framework)[57], the problem is even more significant on a global scale. Currently, a European Parliament and Council regulation proposal that tackles crypto currency markets is being negotiated on the EU level, but the relevant adoption proceeding could take years before a legislative act is adopted and implemented.

Since virtual currency regulation differs between jurisdictions, the jurisdictions do not have a uniform overview of the sector or the capability to exercise control. For example, one party to the transaction is located in a jurisdiction where the transaction participants are not identified or verified, and history of transactions that would be linked with a certain person cannot be submitted or the regulation is weak, information is unavailable for the FIU and tracing the money becomes impossible.
In the situation where the compliance programme is too burdensome from the client's perspective compared to the measures implemented by competitors, the service provider's business becomes unsustainable and unprofitable, the result of which is the closure of business or reduced rate at which the money laundering and terrorist financing prevention measures are implemented.

In addition to the fit and proper tests and other procedural measures, it is also important that the supervisory authority would have the resources to analyse the MLTFPA due diligence measures applied by the activity license applicant, incl. procedural rules and their implementation, because at this time the

[57] Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

respective compliance programme of some service providers that have been granted authorisation does not meet the requirements pursuant to law and the expectations of the legislator and supervisory authority. It is also important to understand if the compliance function of the activity license application, especially the function of the contact person is performed by an official employee with an employment contract or a compliance service provider, the number of whom is remarkable in Estonia. If the role of the contact person is filled by a third party, it is to be expected that the level of compliance and accuracy in terms of time for not meeting the service provider's specific risks and the motivation of a contact person working in such cooperation format is not aimed at managing actual risks or ensuring the good reputation or sustainability of the service provider' activities. To ensure that the expectations of the legislator and supervisory authority are met and understood, it is among else relevant to stress and encourage harmonised cooperation between the state and service providers so that respective expectations would be achievable and in proportion to the specific sector and accompanying threats.
It has also been found that information exchange between competent authorities is complicated, primarily communication with supervisory authorities of third countries.

Pursuant to the fact that Estonia plans to improve the legal environment of virtual assets in 2021, the possibilities of realisation of several above-mentioned threats are mitigated. Also, a proposal for regulating markets for crypto assets has been submitted on EU level which will improve the legislative sphere in the future across Europe.

Adhering to the aforementioned, the threat related to regulative environment can be considered "average".

<u>Criminal activity</u>

- The virtual currency service provider activity license, issued in Estonia by the FIU, is used abroad for providing other financial services that require a respective activity license and the aim is to deceive clients.
- Virtual currencies are used both for paying for illegal transactions and for exchanging "dirty" money.
- The problem is the exploitation of design errors of virtual currencies and the use of virtual assets for ransomware (so-called virtual extortion).
- Digital supply chains make it easy to commit identity theft.
- Creating virtual currency wallets and dividing large sums among several parties is easy, therefore it is difficult to identify money laundering schemes when virtual currencies are in use. Virtual currencies allow the criminals to store assets outside of formal financial system and digitally, to hide its origin and final owner.
- Virtual currencies and assets are popular means of payment in transactions between criminals made in the dark web.
- Computer scams.
- Drug trafficking.

Criminals use FinTech sector for moving their illegally obtained assets at least in one money laundering stage (placement, layering, integration). The aim of the business transactions is to hide the resources with criminal origin and their actual owner. Fast cross-border cashflows from countries that do not participate effectively in international cooperation, give the criminals a chance to direct their resources into legal business.

Money laundering is a criminal offense preceded by criminal offenses involving tangible income (predicate offenses). A few decades ago, only drug related crimes with exceptionally large proceeds of crime were considered as a predicate crime, nowadays basically each crime that generates criminal proceeds can be considered as a predicate crime for money laundering.[58] As cash is anonymous in nature, there is a threat that illegally obtained cash will be placed in the financial sector.

[58] Source: Estonian Banking Association, https://pangaliit.ee/rahapesu-tokestamine.

Cash turnover is rather low in Estonian economy. Avoiding taxes, cash earned with (cyber) fraud and drug and contraband trafficking are threats in terms of cash in Estonia, where financial service providers may come into contact with large amounts of cash of unclear origin that someone tries to hide or direct into the legal economy.

Virtual currency service providers may also provide services to criminals or legal persons who do not comply with regulations, if they do not apply due diligence measures sufficiently. Since virtual currency sector and technology are rapidly developing, it is difficult to ensure sufficient risk awareness and mitigation of all risks.

According to the FIU survey, use of virtual currencies is common in criminal schemes in Estonia and a large part of settlements in the so-called criminal sphere is done in virtual currencies. Virtual currencies are also used in the preparatory phases of criminal offenses. Virtual currencies are used for handling assets acquired through computer scams and drug trafficking.[59]

At the end of 2018, the capacity of illegal transactions reached globally 76 billion USD, i.e. 46% of all bitcoin transactions, the market share of which at the time was more than 63%, that is almost comparable with the US and EU narcotic substances market capacity. It was also found that nearly 26% of all users and 23% of the value of all virtual currency transactions could be related with illegal activities, primarily through the dark web. As of April 2017, it was presumed that 27 million market participants use bitcoin for illegal purposes, making nearly 37 million transactions per year and collectively controlling almost bitcoins with the worth of 7 billion USD. It has been observed that payment practices and user habits of bitcoin users related with illegal activities differ from those of the users acting according to law. For example, if a regular user owns a large amount of bitcoins, they mainly use it for investing. Usually, criminals use bitcoins as a payment instrument due to the risk of getting their assets seized and they might make more transactions in smaller sums and they do transactions more likely with tumblers or mixers and with same partners. For example, bitcoin transactions network between illegals is 3 to 4 times tenser than between regular users.[60]

It is worth mentioning that although in 2019 only 5% of active virtual currency service providers followed the reporting obligation provided in the MLTFPA and of all the virtual currency sector reports 93% were submitted by only 3 market participants, then the aforementioned survey conclusion on criminals using bitcoins is also apparent in the FIU reporting statistics. If unusual transaction reports' (UTR) share in the virtual currency sector reports was non-existent, then reports on unusual activities (UAR) made up 14.1% of all reports. Adhering to the virtual currency service providers being subjected to the same MLTFPA requirements as financing institutions, it can be presumed that money laundering and terrorist financing tools, methods, due diligence measures and quantity and quality of the reports forwarded to the FIU have improved going forward. This is illustrated also by the fact that differently from cash or bank transfers, virtual currency transactions are publicly available in the blockchain and using different screening and monitoring systems and various transaction analysing methods, it is possible to identify the actual origin and the point of destination of virtual currencies.

Adhering to the aforementioned, the threat related to crimes can be considered "average/high".

<u>Conclusion</u>

Virtual currency sector

Although virtual currencies are popular means of payment among money launderers, the virtual currency service providers can identify such persons and transactions by implementing respective investments and mechanisms and also by informing the supervisory authority. Thus, it is found that until now the general

[59] FIU, virtual currency service providers survey, p 19.

[60] S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 26, p 1-3. Available online on this link.
R. HOUBEN., A. SNYERS. European Parliament. „Crypto-assets. Key developments, regulatory concerns and responses.", April 2020, p 25. Available online on this link.

virtual currency sector money laundering threat exists because needed investments, competence and motivation, with the exception of a few service providers, are low in general. There are also shortcomings at the regulative level, both nationally and globally.

Adhering to the aforementioned, the threat related to virtual currencies can be considered "average/high".

7.3.2. Common threats

Possible threats related to crowdfunding:

Threats related to state or geographical location

- Crowdfunding sector is also international and brings together investors and applicants for financing from all over the world. The service provider has a global reach, connecting the interests of investors and project owners who are located at different jurisdictions. Project owner, investor or their respective beneficial owners may be located in jurisdictions that have higher ML/TF risks or lack of effective anti-money laundering tools and lack of supervision for the prevention of terrorist financing. Crowdfunding service providers may be located at any place in the world, incl. high-risk regions[61].
- Funds are received from personal or business relations with a jurisdiction in which case reliable sources have identified significant connections with corruption or other criminal activity such as terrorism, money laundering, illegal drug production and trafficking or other predicate crimes.

Analysis of realisation of a possible threat in Estonia:

Nearly 60% of projects financed by Estonian crowdfunding companies take place in Estonia and 40% abroad. Estonian share decreases over the time, because entrepreneurs expand abroad, this is also promoted by the EU's implementation of the crowdfunding regulation from 10.11.2021, which gives the service providers the chance to operate in the EU under same requirements and with a single activity license.

Adhering to the aforementioned, the threat related to state or geographical location can be considered "average".

Threats related to services, product features and transactions, and distribution channels

- Crowdfunding services are provided online via web portals.[62]
- In case of equity and credit-based crowdfunding it is possible to raise larger sums (risk is higher than with donation-based crowdfunding), although in general such platforms are regulated (incl. disclosure requirements and use of credit institutions).
- Crowdfunding service provider accepts cash investments on the platform or allows withdrawing cash from the platform.[63] Some crowdfunding service providers allow to invest also into crypto assets or make payments with the mentioned assets via the crowdfunding platform.[64]

[61] Sectoral guideline for regulated crowdfunding platforms (Guideline 17), https://eba.europa.eu/calendar/draft-guidelines-under-articles-17-and-184-directive-eu-2015849-customer.

[62] ACAMS, Crowdfunding: The New Face of Financial Crimes?, http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf. Estonian FinTech sector vulnerabilities, document analysis, p 39.

[63] Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37, Guideline 17, p 125, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%20%28EU%29%202015/849%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf.

[64] Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with

- Crowdfunding service provider allows to make transactions on the platform between investors or project owners, or allows investors make a payment to the project owner via platform using instruments which are not regulated or for which less strict AML/CFT are imposed in comparison with Directive (EU) 2015/849.
- The crowdfunding service provider does not limit the size, capacity or value of transactions processed using the crowdfunding platform, the loading or redemption processed using the crowdfunding platform or the amount of funds stored on single investors' accounts.
- Crowdfunding service provider allows early redemption of investments, early repayment of loans or resale of investments or loans via aftermarkets, also leverage or privileged redemption or guaranteed rate of return.
- In case of credit-based crowdfunding there is understandably no nominal interest rate, interest payment date, interest payment deadlines, deadline and implemented rate of return provided.
- Crowdfunding service provider allows the investors and project owners hold multiple user accounts on the crowdfunding platform.
- Crowdfunding service provider manages the crowdfunding platform fully online without sufficient protective measures, e.g. electronic identification, using electronic signatures or electronic identity documents which comply with regulation (EU) 910/2014. Clients are accepted or on-boarded without face-to-face identification and the protective measures are not set.
- Crowdfunding service provider offers its services outside of any regulations and thus measures that would identify or mitigate the risks concerning the crowdfunding service provider being used for money laundering or terrorist financing may not be implemented.
- In case of crowdfunding service providers the risk factors are: the platform allows transferring money later on (e.g. collecting money for an unknown project or returning money to investors), capability of reselling investments, platform does not set limits for transactions, it is possible to make payments using unregulated or under regulated currencies, platform allows cash deposits and withdrawals, platform does not allow repurchases, platform payments can be made in virtual currencies, allows clients to manage multiple accounts that are not connected to each other.[65]

Analysis of realisation of a possible threat in Estonia

In general, for the provision of the services crowdfunding service providers must use a payment account offered by credit and payment institutions, for example. Since credit institutions are strictly regulated, using their services helps to mitigate certain threats. Thus, the service providers are interested in having correct processes that help to manage the threats present in financial technology sector to meet the requirements set by the person who provides the payment account service.

Adhering to the aforementioned, the threats related to services, product features and transactions and distribution channels can be considered "low/average".

Threats related with clients

- The complexity related with identification and determining the beneficial owner (service provider is unable to identify the transaction the other party of which is a PEP, due to the shortcomings in either screening system or PEPs' list, the service provider is unable to identify the beneficial owner because of the complicated owner structure of the client or other party of the transaction, or lack of information on beneficial owners in the register).
- The non-resident or e-resident clients (service provider cannot implement appropriate due diligence measures for clients who are non-residents or e-residents).
- The investor requests privileged conditions or fixed investment profitability or askes to repurchase the investment in a short time after initialling investment or transferring funds to the platform that exceed the sums needed for the project and then asks to refund the excess amount. Origin of the funds meant for investing is unclear and the investor does not want to submit this information when requested. Level of invested assets exceeds in estimation the investor's liquid

individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37, Guideline 17, p 126.

[65] EBA acts to improve AML/CFT supervision in Europe, https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terroristfinancing-risk-factors.

assets capacity. The invested funds are burrowed. The investor refuses to submit required data that is necessary for the service provider to conduct appropriate due diligence procedure for the client.

- The applicant's business plan (investment project) has no obvious strategy or economic purpose. The applicant accelerates unexpectedly or without a reasonable explanation the agreed redemption or repayment schedule, either by a single payment or early termination. The applicant seems to be against submitting information on the project or its owner.

Analysis of realisation of a possible threat in Estonia

There are no known problematic issues with identification of Estonian clients. But since it is an international sector, identifying clients might be problematic on a global scale. There are shortcomings in the use of identification technology and elsewhere. At the same time, the majority of transactions take place in Estonia that is why the threat is certainly smaller than in case of virtual currency service providers. Threats also exist in building customer relationships, where greater misuse of identification documents is a problem. Smaller service providers may have problems with identifying non-resident clients in the desired extent and thus the funds, the origin or owner of which is unclear, may end up in the FinTech sector. By implementing suitable due diligence measures on clients, it is possible to keep the FinTech sector clear of people who might abuse it.

Adhering to the aforementioned, the threats related to clients can be considered "low/average".

Threats related with regulative environment

- Domain-based regulations are still in development, which allows the service providers to operate under limited supervision or without it. The risk is also seen in the fact that new regulations have been introduced mainly for equity-based platforms (raising capital from investors through the sale of shareholdings) and thus leaving the financial industry open to risks of fraud, money laundering and terrorist financing.[66]
- Currently, provision of crowdfunding may not be under financial supervision and the service providers and applicants do not have to submit mandatory reports or information. Thus, the information obtained on the project may be limited.[67] In several EU member states the crowdfunding service providers are not regulated or there are only certain categories created.
- Crowdfunding service providers are not handled as obliged entities in terms of money laundering and terrorist financing prevention regulations.

Analysis of realisation of a possible threat in Estonia

In 2021, the plan is to regulate the crowdfunding sector of Estonia, incl. setting respective activity requirements, activity license obligation and supervision. For more information, see the section about the legal framework of crowdfunding.

Adhering to the aforementioned, the threats related to regulative environment can be considered "low/average".

Criminal activity

- Crowdfunding companies have been established in Estonia with the purpose of committing an investment fraud because regulation is insufficient and the process of establishing a company is easy/simple and relatively cheap.[68] Frauds and abuse of of investors' trust are frequent (e.g. fictitious projects the goals of which are never reached).
- A threat could also be the risk of crowdfunding platforms established by organised crime or use of undercover agents.

[66] ACAMS, Crowdfunding: The New Face of Financial Crimes?, http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf. Estonian FinTech sector vulnerabilities, document analysis, p 39.
[67] Estonian FinTech sector vulnerabilities, document analysis.
[68] See https://www.politsei.ee/et/uudised/kas-envestio-ja-kuetzal-puhul-oli-tegemist-pettusega-1151.

Analysis of realisation of a possible threat in Estonia

At this time, realisation of the aforementioned threats may be average/high. Crowdfunding companies have been established in Estonia with the aim of committing an investment fraud because regulation is insufficient and establishing a company is easy/simple and relatively cheap. For example, in 2019 and 2020 frauds were committed in relation to the provision of crowdfunding services. In several cases, it was a company established in Estonia by an e-resident, who had no other connection with Estonia, the company's activities were also managed from abroad.[69]

Adhering to the aforementioned, the threats related to crime can be considered "average".

Conclusion

Crowdfunding sector

Probability of threats related to money laundering occurring in Estonian crowdfunding sector is rather low. The sector is small and the capacity of mediated transactions remain marginal. So far, no money laundering cases related to the provision of crowdfunding service have been identified in Estonia.

Adhering to the aforementioned, the threats related to clients can be considered "low/average".

7.3.3. Terrorist financing threats

Common threats

Common risk scenarios in the virtual currency sector:

- It is easy to move virtual assets on the global level.
- Threats related to the nature of virtual assets, incl. (pseudo) anonymity[70] and speed, opportunity to use online and as a cross-border service, anonymous access to assets, possibility to hide transaction history, owning private keys and option to use ATMs. Terrorist organisations publicly call to support their activities either in a combined manner "payment service provider + virtual currency" or just in virtual currency to ensure maximum anonymity in transactions.
- Using virtual asset mixing services allows more privacy, faster transfers, lower transfer fees and smaller price fluctuations.
- Insufficient knowledge of terrorist financing among the service providers may cause insufficiency of due diligence implemented for terrorist financing.
- Although starting from 10.03.2020, the same MLTFPA requirements are valid for virtual currency service providers as for financing institutions, there are still problems with complying with the know-your-client or KYC requirements. Thus, there is a threat that a service is provided for example to sanctioned persons because of terrorist financing. In general, no face-to-face meeting happens in providing virtual asset service, which in turn may allow anonymous financing or purchase of products (cash payments or payments by third persons that do not recognise the origin of the resources) in a situation where the service provider does not implement the appropriate due diligence measures. Anonymous transactions are also considered as a threat, if the sender and receiver are not appropriately identified.
- Issues with awareness of risks, among else of what methods terrorist organisations use in abusing cryptocurrency and in the related technical resources to collect, transfer or store money, also exist with no doubt on institutional level, that is why the regulative environment may not always meet the expectations of a real life. Thus, technological developments offer the sector and the regulators new challenges in the fight against terrorist financing.
- Since virtual currencies and assets are popular means of payment in transactions between criminals, it can be presumed that there is a threat that these may also be used in terrorist financing. At the same time, the FIU admits in its survey that the number of confirmed cases on terrorist financing using virtual currencies is rather small. Cases have been identified where Islamic or extreme right groupings have used virtual currencies to buy illegal items (such as

[69] See for example https://www.politsei.ee/et/uudised/kas-envestio-ja-kuetzal-puhul-oli-tegemist-pettusega-1151. See also ECN reports Kuetzal and Envestio to National Conduct Authority, https://eurocrowd.org/2020/01/22/ecn-reports-kuetzal-and-envestio-to-national-conduct-authority/.

[70] Anonymity and pseudo-anonymity (using certain technology it is possible to identify the actual user).

weapons) from the dark web, raise capital on crowdfunding platforms or to move assets internationally (P2P or peer to peer transactions). Thus, the virtual currencies gain popularity among Islamic extremists who use them for organising money raising campaigns by sharing anonymous wallet addresses via social media or chat applications.[71] Using efficient transactions screening and monitoring mechanisms it is possible, regardless of aforementioned, for the virtual currency service providers to quite efficiently identify such addresses, halt the transactions and share the respective information to the FIU.

Common risk scenarios in the crowdfunding sector:

- Although crowdfunding websites are not completely new, they pose an additional risk, because they are created especially for obtaining financing and donations. In 2015, the European Securities and Markets Authority (ESMA) highlighted the threat from investment-based crowdfunding: these could be abused for financing terrorism, especially if the platforms perform the due diligence measures in terms of the project owners and their projects in a limited extent or not at all.[72]
- One risk typology is abuse of the donations-based crowdfunding service for terrorist financing. Abuse of the charity donations for terrorist financing is one of the main financing channels for many terrorist organisations. The Financial Action Task Force (FATF) has published concrete instructions for this topic in recommendation 8.[73] Cases of misuse of crowdfunding websites have been identified for charity purposes which actually benefitted terrorist organisations.[74] The challenge for legislators and competent authorities is lack of information for the assistance of the campaigns on these platforms.[75]
- Special attention should be paid to jurisdictions that are known for financing or supporting terrorist acts or where it is known that groups committing terrorist acts operate, and at jurisdictions for which financial sanctions, embargos or measures (issued by the EU or the UN, for example) that are related to preventing terrorism, terrorist financing or spreading, are enforced.

7.3.4. Conclusion

Because of its location and small Muslim community, Estonia is not the first target for terrorist acts committed by Islamic extremists. At the same time, close neighbours such as the Scandinavian countries and Russia have large Muslim communities and that is the reason why many persons with extreme Islamic views use Estonia as a transit country. Favorable economic environment and real estate market of Estonia have sparked business interest also in the aforementioned communities. The threat of terrorism from other sources is very small compared to Islamic terrorism.

The innovative and developed FinTech sector of Estonia may become increasingly attractive for Islamic extremists from the point of financing and supporting terrorism. Among the people and groups with extreme Islamic views the traditional channels for funding terrorism are being replaced with alternative financial service providers. Virtual currencies may also ensure complete anonymity.

[71] See also ACAMS, New Technologies: The Emerging Terrorist Financing Risk, 03.06.2020, https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.
[72] Questions and Answers: Investment-based crowdfunding: money laundering/terrorist financing, European Securities and Markets Authority, 1 July 2015, https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2015_1005_qa_crowdfunding_money_laundering_and_terrorist_financing.pdf.
[73] Risk of Terrorist Abuse in Non-Profit Organisations, Financial Action Task Force, June 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf.
[74] APG/MENA FATF Social Media and Terrorism Financing Report, 23 January 2019, Asia/Pacific Group On Money Laundering, http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142.
[75] Alexandra Posadzki, "Hard to identify crowdfunding platforms financing terrorism," The Star, 18 May 2017, https://www.thestar.com/business/2017/05/18/hard-to-identify-crowdfunding-platforms-financing-terrorism.html.

The FIU has received reports from virtual currency service providers where sanctioned persons related with terrorism have wanted to establish business relations, which is a clear indicator that virtual currencies are attractive in terms of terrorist financing.

Also, application of enhanced due diligence measures only when transaction limits are exceeded is no longer appropriate or efficient. Majority of transactions with suspected terrorist financing are made using small sums (also under 10 euros). Investing such sums is easily allowed by the crowdfunding sector, incl. donating small sums using donations-based crowdfunding platforms.

Based on the aforementioned the terrorist financing risks related to virtual currency service provision can be considered rather "high", risks related with crowdfunding service provision as "average".

7.4. Vulnerabilities

7.4.1. Vulnerabilities of prevention of money laundering

In this NRA, the **money laundering vulnerability level** of FinTech sector was assessed[76] as follows:

Table 38. Money laundering vulnerability levels in FinTech subsectors

FinTech sector	**Money laundering vulnerability level on sectoral level**	
Virtual currencies	**3.02**	average/high
Crowdfunding	**1.99**	average/low

Virtual currency sector

Virtual currency sector involves the following vulnerabilities:

- The supervisory authorities do not have sufficient resources (human, IT, legal and time) to substantially execute control over compliance of companies headed for the virtual currencies market. From 2019, the FIU hired more employees (9 people in total who work on supervision and issuing activity permits) to better manage the rapid growth in workload from virtual currencies license applications in 2018-2019. From March 2020, the extent of the object of control of the activity license changed, the processing time of activity license extended to 60 days, state fee rose to 3,300 euros, required share capital increased to at least 12,000 euros and the requirement of a contact person was established. These additional measures may organise the market, but this has taken place in the state with a long delay. The measures should be taken continuously more effective because it is not understandable how more than 400 virtual currency service providers could fit the Estonian market so that all of them could comply with the supervisory and preventive measures and remain that way. It must also be analysed what could be the competent authority in the future to issue the respective activity licenses. The mentioned obligation needs to be covered with sufficient resources as well.
- The supervisory authorities do not have sufficient resources to carry out also risk-based supervision on a level that would provide information on the companies operating in the sector and removing licenses from persons not complying with the requirements if necessary. Also, it is impossible to conduct supervision over companies with new activity licenses so that first it could be identified if the company has started operating or not and then accordingly clean the market of companies that do not need activity licenses for operating. Thereby, it would be possible also to reduce the threat of misuse of activity licenses. There is an insufficient time resource in the supervisory authorities because everyone is busy either with issuing activity licenses or conducting on-site control. Upon lack of efficient supervision the threat that the virtual currency sector is used for money laundering may realise.

[76] Assessments given by the NRA threats working group, which are based on the risk assessment performance method.

- Anonymity – from 10.03.2020, the virtual currency service providers are prohibited to provide anonymous services (§ 25, subsections 1 and 2 of the MLTFPA). This means that sporadically when making transactions and establishing business relations, the client must be identified and the submitted information must be checked regardless of the transaction sum. Nevertheless, there is the threat that the service providers do not follow the requirements provided in the law and the customer/client is not (properly) identified.
- The feedback provided to virtual currency service providers revealed that in 2019, only 8 sector reports were sent to in-depth analysis and information on 7 reports was forwarded to competent Estonian investigative authorities, because the majority of persons included in the report do not have a connection to Estonia and they are foreign citizens. A vulnerability could be conducting in-depth analysis for only a few reports but also the situation where the report does not reveal for any reason the actual reason for submitting it or all the important reasons are not highlighted. Thus, everything related to submission the reports could use more precise analysis in the future.
- Using mixing services allows more privacy, faster transfers, lower transfer fees and smaller price fluctuations. This service also allows mixing illegally obtained virtual currency with legal, which is why it is difficult or even impossible to identify the asset movement.
- If the share of cash in the sector is small, then the virtual currency service provider client portfolio from which only 0.15% are persons from Estonia, has a considerable impact on the risk concerning Estonian financial sector. At the same time the statistics is from the FIU survey from November 2019, when 1,282 activity licenses were issued for exchanging virtual currency for money and 1165 activity licenses for providing virtual currency wallet service, there were 1,308 unique companies. As at 01.08.2020 due to the equalization of virtual currency service providers with financial institutions, a total of 611 different virtual currencies activity licenses were valid (295 activity licenses for exchanging virtual currency for money, 261 for wallet service and 55 for virtual currency service). As at the end of 2020, there were 419 virtual currency service providers operating in Estonia. Since the previous law amendment prohibited the virtual currency service providers from providing services outside of business relationship and subjected them to the EEA origin restrictions pursuant to section 31 of the MLTFPA, it can be concluded that the risk related to non-residents, especially clients with a greater risk, is in a considerable decline and the share of Estonians, incl. persons from other EEA member states, is increasing in the client portfolio of the market participants.
- Buying and selling virtual currencies in cash via ATMs in which case identification is incomplete.
- Information exchange between different law enforcement authorities and the FIU is not automatic, but it depends on the interest of the specific investigator to forward the information. The FIU cannot find out in which criminal matters the assets obtained illegally are converted into virtual currencies or which crimes are committed using only virtual currencies. Thus, it is impossible to obtain operative information on companies with the FIU's activity licenses who have breached the requirements of the MLTFPA or who are suspects or accused in criminal procedures. Information exchange is not automatic also in case of international letters rogatory which are also used to request information on companies with Estonian activity licenses. Forwarding of the aforementioned information should take place in the country using digital means, not manually, to speed up the analysis of information.
- Companies established in Estonia and holding activity licenses are committing frauds outside of Estonia, the finances involved in their crimes do not pass through Estonian financial system, the majority of the victims are not Estonian persons. This, however, is an issue in terms of conducting a criminal procedure concerning the activities of these companies, because the fact that the criminal company or its management board member is of Estonian origin is not sufficient to launch a criminal investigation in Estonia. This limits the possibilities to identify using criminal procedural measures the possible connections of Estonian criminal groups in committing the crimes, incl. money laundering or offering money laundering services precisely via Estonian legal persons.

Crowdfunding sector

The vulnerability of money laundering prevention is average-high because the following vulnerabilities exist:

- Until now the sector has been mostly unregulated and unsupervised. In 2021 however several law amendments are planned for the domain (EU's crowdfunding regulation is implemented, additional investor protection requirements for consumer credit-based crowdfunding services are planned to be enforced nationally and economic activity registration obligation for donations- and rewards-based crowdfunding services).
- Little knowledge of the origin of raised funds, extent of crowdfunding and its aim (incl. not publication obligation).

7.4.2. Risk awareness

General risk awareness

Virtual currency sector

Since virtual currency sector and technology are rapidly developing, it is difficult to ensure sufficient risk awareness and mitigation of all risks. Because virtual currency regulations vary per countries, the states do not have a common overview of the sector. The global scale of virtual currency makes conducting supervision and investigation by law enforcement authorities difficult. Thus, risk awareness cannot be presumed because the competent authority needs information on transactions, assets used in the transactions, wallets and beneficial owners of the transactions to perform substantial analysis. Since transactions are cross-border and the service providers are located in several jurisdictions, it is difficult to determine to which jurisdiction the performed transactions belong and how to ensure availability of the respective information. Those virtual currency managers who are located in countries with insufficient money laundering and terrorist financing prevention laws are also considered as a vulnerability. It is also complicated to restrict the forwarding of virtual currencies and demanding data from the obliged entity. Additionally, the fact that a virtual currency service provider is registered, brings more trust in the customers, which allows fraud and embezzlement of customers' assets.

The lack of legislation or its insufficiency can be considered the main vulnerability. There is also currently no wider regulation that would regulate virtual assets in a wider sense. The MLTFPA presents a definition for virtual currency which is too narrow for newer virtual assets because the newer virtual assets do not fall under the definition provided in the law and are thus not subject to the regulation either. The use of tokens is increasingly popular, and they are not covered by the virtual currency definition. Ministry of Finance has published a draft legislation (ACOIIVC)[77] with which they want to also regulate those crypto assets and crypto asset service providers that are not subject to the currently valid MLTFPA. This draft act outlines requirements for instruments that have an investment object or are associated with the holding of a share in a legal entity/person or the carrying out the control in another legal entity/person in another manner.

According to the draft act, the plan is also to enforce requirements for the service provider who organises the virtual currency trade platform.

The survey results of awareness:

The results of the survey conducted within the NRA indicate that the sector's awareness on preventing money laundering is rather modest (see also the following aspects). Also, less than half of the service providers do not assess the employees' reliability during the working relationship, therefore the employer does not know if all money laundering prevention principles are followed.

[77] Draft Act on Crowdfunding and Other Investment Instruments and Virtual Currencies – see text in legal framework chapter.

The survey results of the reporting statistics:
The sector performs its reporting obligation modestly. 6% of the survey respondents had not or did not know if the company had developed a methodology and/or a guide for reporting suspected ML and TF or unusual transactions. At the same time, the service providers are obligated to enforce a methodology and instructions if suspicion of ML and TF arises or if an unusual transaction or circumstance occurs, and instructions for following the reporting obligation. The survey also revealed that more than half of the service providers have not needed the guide in practice yet. Considering the annual turnover of the survey respondents, it is suspicious that with turnovers on this level, the companies have not faced circumstances that should have been reported to the FIU. This hints that the service providers do not follow the reporting obligation and do not forward many important reports and suspicions to the FIU, that is why the FIU does not have the necessary information for identifying the risks and schemes spreading in the sector.

According to the methodology, the working group assessed the vulnerabilities related to the knowledge of ML prevention belong the employees of the virtual currency service providers as high. The general risk awareness of risks that exist in the sector is low.

Crowdfunding sector
Risk awareness in the crowdfunding sector can be considered average at this time. The low level of knowledge may be due to insufficient regulation of the sector, but in 2021, the EU crowdfunding regulation is implemented, and the national sector-specific legal environment will also be enhanced. In relation to the aforementioned, the effective investor protection is also enforced that will surely make the activities of entrepreneurs more transparent. Considering that this sector has also received media attention over the past years, the society's awareness of the sector is no doubt on the rise. The investor-bloggers who write topics related to crowdfunding also contribute to this rise.

There are several active crowdfunding service providers in Estonia who voluntarily comply with normal financial sector requirements and who do it among else with the aim of applying for the respective activity license in 2021 or following years for providing crowdfunding service. Several of them also follow the crowdfunding good practice guidelines prepared by NPO FinanceEstonia, which, according to the survey feedback, has been helpful for the service providers[78]. According to the survey, about half of the respondents have found the referred guideline useful. More than half of the respondents have also found the FIU's instructions useful. The majority of the survey respondents have enforced internal rules according to section 14 of the MLTFPA although the law does not provide such obligation for them. This is likely pressure from the business culture (e.g. pressure by credit institutions).

Survey results of awareness:
Results of the survey conducted within the NRA show that sector's awareness of ML prevention is rather good.

Survey results of the reporting statistics:
71.4% of respondents are of the opinion that reporting of suspected money laundering does not bring any negative consequences for the employee who filed the report. This is positive and indicates awareness of how responsibility is distributed on the company's level in case of reporting. At the same time, 28.4% of respondents believe that reporting of money laundering suspicions might bring negative consequences for the company. In the fear of negative consequences, the companies may choose not to report the suspected money laundering, which in turn may raise the sector vulnerability level.

According to the methodology, the working group assessed the vulnerabilities related to the knowledge of ML prevention belong the employees of the crowdfunding service providers as

[78] Nearly half of the respondents have found this useful.

low/average. The survey questionnaire results were also considered when giving the assessment, according to which the majority of the respondents provide their employees with respective training, offer web courses and raise the general awareness level consistently. Based on the aforementioned, the general risk awareness of risks in the crowdfunding sector is average.

Commitment of management and leader role

Virtual currency sector

The survey results indicate that risk awareness in the virtual currency sector is low and needs enhancing. The results show that Estonian virtual currency service providers have had no contact with enforcement measures of foreign authorities, thus, these rather have no impact on the Estonian service providers. Although clause § 72, subsection 1, clause 5 of the MLTFPA states that the virtual currency service provider must have a settlement or payment account, it is presumed that the payment account is created with a foreign payment service provider, which raises the risks of the service provider, screening and supervision.

To conclude the survey, it can be said that the comprehensiveness of the "know-your-employee" programme is rather lacking and the employers do not know their employees sufficiently, which creates a high risk. Cooperation with the Security Police would also help in screening the employees, because obtaining the necessary information is difficult for the obliged entity. Since slightly less than half the service providers do not assess the employees' reliability during the professional relationship, the employers experience unawareness regarding following the ML prevention principles. Also, almost all survey respondents breach the confidentiality requirement. The FIU has the right to control the contact person candidate's fit for performing the tasks provided in the law when processing the activity license application. When conducting supervision, it is checked if the obliged entity has followed the requirements pursuant to law when providing the service and who was responsible for the claims from the MLTFPA. Also, nearly 80% of the survey respondents find that reporting suspected ML will not bring negative consequences for the employee and although some companies use different mechanisms, it can be presumed that in the majority these are absent or that there are significant shortcomings and they do not receive much attention.

Management commitment and leadership was assessed according to the methodology in three subclauses, the vulnerability assessments of which were the following:

- pressure from the market to follow ML prevention standards – high;
- presence and efficiency of internal control – average/low;
- honesty of employees – average.

Crowdfunding sector

Since the market participants generally cooperate with credit institutions, some market participants implement due diligence measures provided in the MLTFPA (due to so-called business culture). It would not be possible to own an account via which one can raise money without cooperating with a credit or payment institution. Risk awareness can be assessed as average.

The majority of the respondents (78.6%) conduct background check when hiring employees. This fact reduces the sector's vulnerability. For background check, public registers (38.1%), Google and social media (21.7%) and recommendations (19%) are used the most. Statements from the criminal records (9.5%), contact with previous employers (9.5%), credit history check (4.8%) and resumes (4.8%) are used less. The principles of those market participants who conduct reliability assessment during employment relationship (35.7%) include observation and control over employee activities (40%) and interviews with the employee and filling in questionnaires (20%).

14.3% of respondents have confirmed that they do not have a regular training plan and they are not doing anything to ensure that employees responsible for preventing money laundering in Estonia would receive regular training. Vulnerability is low because the majority of market participants provide trainings and web courses for this purpose (57.1%) and raise the general awareness (21.4%).

In case of just 3 respondents, the employees have not passed a money laundering prevention training over the past three years. In case of the rest of the respondents, 1 to 3 employees had received training and in two instances all employees had been schooled. Passing a training course reduces vulnerability and raises awareness. 46.7% of market participants ensure with trainings that the employees would be aware of ML prevention obligations. Others use different measures. At the same time, 57.2% of respondents either do not know any measures (14.3%) or do not use any measures (42.9%) to protect the employees connected with ML prevention obligation from the negative consequences related with the activity. This shows that more than half of the respondents do not think about how the employees working with ML prevention could perform the task of ML prevention as objectively and safely as possible. The aforementioned is a certain indicator of vulnerability. Nevertheless, 71.4% of respondents are on the opinion that reporting of suspected money laundering does not bring about negative consequences for the employee who filed the report. This is positive and indicates awareness that reporting is not refused due to the possible harm to the employee, i.e. they are aware of how responsibility is distributed on the company level in case of reporting. Vulnerability is very low in terms of the aforementioned. 28.4% of respondents believe that reporting of suspected money laundering might bring about negative consequences for the company. This, however, indicates some vulnerability because in case of possible negative consequences for the company, reporting may be avoided.

Management commitment and leadership was assessed according to the methodology in three subclauses, the vulnerability assessments of which were the following:

- pressure from the market to follow ML prevention standards – average/low;
- presence and efficiency of internal control – average/high;
- honesty of employees – average.

7.4.3. Legal framework and control

General

Virtual currency sector

Before 10.03.2020, the activity licences of virtual currency service providers were distinguished by two services: exchanging virtual currency for money and virtual currency wallet service. From the mentioned date, the two activity licences are considered equal to the activity licence of a virtual currency service provider, i.e. there is a single comprehensive activity licence.

The new wording of the MLTFPA that was entered into force on 10.03.2020 substantially amended the requirements the state presents to the virtual currency service providers. The amendments included, among else, nearly five-fold growth of share capital and the requirement that the company's place of business and location would be in Estonia. The aim of the amendment was to enhance the activity license conditions for virtual currency service and wallet service providers to reduce the ML and TF risks related to these services.

The stricter requirements did not concern only new entrepreneurs. During the transfer period which lasted until 01.07.2020, all service providers already holding the respective activity license also had to make sure their activities and documents comply with the requirements. If the entrepreneurs did not perform the provisions of subsection § 118^2, subsection 1 of the MLTFPA by the given deadline, the FIU revoked their activity licenses.

The entrepreneurs had to consider the following in complying with the activity license:

- Requirements concerning the entrepreneur's location: the company's registered location, location of the management board and place of business must be in Estonia. If a foreign company operates in Estonia via a branch registered in the Estonian commercial register, its place of business and physical location of the manager must be in Estonia. According to statistics, the majority of the companies with the activity license are non-residents. This means that in order to comply with the activity license requirements, a foreign entrepreneur must establish a branch in Estonia.

- Share capital size requirement: the company's share capital must be at least 12,000 euros. Share capital must be paid fully in money.
- Payment account requirement: the entrepreneur must own a payment account at a credit institution, e-money institution or a payment institution that is established in Estonia or in a European Economic Area member state and provides cross-border services in Estonia or has opened a branch in Estonia. To comply with the new wording of the activity license requirements, the entrepreneur must submit to the FIU a list of all payment accounts on its name with each payment account's non-recurrent identifier and account holder name.
- Proof of the entrepreneur's background, suitability and correct good reputation: the company should submit documents on its managerial body member and procurator that indicate education level, full list of job positions and in case of managerial body member also the area of responsibility. Since a similar requirement is also included in the current act, many entrepreneurs have probably already submitted the mentioned documents along with activity license application. Thus, each entrepreneur should check which documents have already been submitted when applying for the activity license and then assess which additional documents should be submitted, if any. The entrepreneur must also submit other documents they consider important in proving the good business reputation of their managerial body member, procurator, beneficial owner and owner.
- Identification documents and documents proving absence or criminal punishment: if the entrepreneur, its managerial body member, procurator, beneficial owner or physical person owner is a citizen of a foreign country, copies of identification documents from all countries of nationality shall be submitted to the FIU. Also, in this case criminal records database proofs or an equal document issued by a competent judicial or administrative body that proves absence of punishment for a crime committed against the state or a money laundering related offence or any other intentional crime must be submitted from all countries of nationality. By the time of submitting the proof not more than three months can be passed from the issuing of the proof. The proof must be authorised by a notary or in an equal format and legalised, or confirmed with a certificate that substitutes legalisation.
- Virtual currency service providers are mandated to record the respective provisions of money laundering and terrorist financing prevention in their principles of action or rules. Although 85% of the respondents find that procedure rules have been reviewed over the past year, it is questionable whether it is done all the time, is this adhered to in one's activities and is it done according to the identified risks and, in turn, to the ML/TF risk assessment.
- Entrepreneurs are obligated to submit data that confirms their knowledge, skills, experience, education, professional competence, and impeccable business reputation. A company's contact person must also work permanently in Estonia (subsection 17 5) of the MLTFPA). The data submitted on the person's suitability must be comprehensive and sufficient and adequately reflect the suitability of the person, which the FIU has a right to check when processing the activity license.
- According to the MLTFPA amendment enforced on 10.09.2020, virtual currency service providers are considered financing institutions which is why requirements pursuant to MLTFPA section 31 apply for them in terms of identification and checking data using digital means.
- On 15.01.2021, the Ministry of Finance published the draft Act on Crowdfunding and Other Investment Instruments and Virtual Currencies.

Although vulnerabilities related to legal framework are assessed as average/high, the respective Estonian regulations have been repeatedly enforced over the past years and the legislator is also planning law amendments in the near future that mitigate the risks in this sector even more.

Crowdfunding sector

At this time, the crowdfunding service providers do not have an obligation for a license or registration to provide crowdfunding service, excl. in case of certain business models, which may require an activity license from a creditor, credit intermediary or investment association. The number of crowdfunding service providers interviewed within the FinTech sector is 34, the majority of whom

(82.4%) are not obliged entities in the sense of the MLTFPA. On 10.11.2020, the EU crowdfunding regulation was adopted, which will be enforce from 10.11.2021. In January 2021 the crowdfunding and other investment instruments and virtual currencies draft legislation was also published, which is planned to be enforced on 1 July 2021. The referred draft act will regulate matters in which the EU crowdfunding regulation provides legislation or sets an obligation and specify requirements for crowdfunding models that are not in the scope of the EU crowdfunding regulation. For example, according to the proposal, the crowdfunding service providers that intermediate consumer credit must in the future also meet the investor protection requirements, the plan is also to set mandatory economic activity registration for donations- and rewards-based business models. Also, the crowdfunding service providers must start following the MLTFPA requirements.

Vulnerabilities related to the legal framework of crowdfunding are assessed as average. When assessing the vulnerability, it was considered, among else, that EU crowdfunding regulation will be implemented from 10.11.2021 and certain changes are also planned nationally (see previous comments on the ACOIIVC draft act). Additionally, many service providers follow the good practice of the sector and other requirements voluntarily.

Supervision quality

Virtual currency sector

Since until now, supervision has been rather one-sided, i.e. it has been only about data inquiries and revoking activity licenses, the general due diligence and management commitment in the fight against ML and TF has been rather low. The number of on-site checks is marginal and rather insufficient compared to the number of service providers. The number of remote checks could also be higher.

Table 39. The number of virtual currency service activity licenses and the number of conducted checks in years 2018-2020.

Activity licences issued	**as at 31.12.2018**	**as at 31.12.2019**	**as at 31.12.2020**
Virtual currency exchange for money	553	1188	31
Virtual currency wallet service	516	1083	29
Virtual currency service	0	0	419

Checks conducted	**2018**	**2019**	**2020**
Number of on-site checks	3	5	7
Number of remote checks	23	29	5

Vulnerabilities related to virtual currency service providers supervision have been assessed as average:

- the existence and implementation of a punishment – average,
- the efficiency of supervision and practices – average.

Crowdfunding sector

Supervision quality cannot be assessed at this time, because there is no regulative control mechanism and a competent authority which is why according to the methodology, the vulnerabilities related to supervision quality may be considered high. In 2021, respective amendments to the legal environment are planned.

Efficiency of compliance control systems and reporting

Virtual currency sector

Market participants should regularly assess the sufficiency of compliance control systems. The survey results indicated that 89% checks the sufficiency of compliance programme, incl. nearly 89% at least

once a year and 30% conducts IT system audits. There is nevertheless a risk that certain number of service providers do not assess the sufficiency of systems regularly. Similarly, it is questionable whether the systems of third person service providers are checked at all or at least on the level declared.

There are various IT solutions available to automate monitoring systems, primarily in case of a large number of clients. Responses to different monitoring systems (for suspicious activities and for financial sanctions screening) indicate that use of automatic systems is not very common. Only 16% of the respondents use automatic system for identifying suspicious transactions and 10% for screening against sanctions lists. Since these are virtual currencies the transactions of which are practically impossible to monitor without automation, there is the risk that a large number of virtual currency service providers possess monitoring systems with significant shortcomings and matters which should be reported to the FIU are not identified.

Virtual currency service provider must also determine a person's risk profile when implementing due diligence measures, considering the prepared risk assessment and matters specified in the law. The survey results indicate that only 40% of the respondents consider the geographical aspect in calculating the risk level and only 41% of market participants use a client risk score.

According to MLTFPA, the virtual currency service provider must enforce an instruction in procedure rules on how to efficiently determine if it is a politically exposed person and upon implementing due diligence measures information must be gathered on whether a person is a politically exposed person (PEP), their family member or a person known to be a close associate. Whereas the law does not provide monitoring frequency. The survey results indicate that a quarter of respondents find that the sources used at the company for identifying politically exposed persons are not sufficient and additional measures are not taken. The survey results also indicate that politically exposed persons are identified only with the necessary diligence.

Within the survey, the convenience of use of mechanisms for reporting suspicious activities were also assessed. In case of the FIU, this is the respective web-based reporting form. Nearly 40% of respondents find that the mechanism for reporting a suspicious activity to the FIU was not user-friendly or they did not comment. Pursuant to this, there is the risk that the companies do not submit reports because the reporting form seems too complicated or time-consuming. At the same time, there is a small percentage of those who would want to integrate the reporting mechanism with their own platform.

Vulnerabilities related to virtual currency service providers compliance control have been assessed as high:

- the efficiency of compliance ensuring systems – high,
- the efficiency of monitoring suspicious activity and reporting it – high.

Crowdfunding sector

Efficiency of compliance control systems and reporting cannot be assessed because there is not regulative obligation. At the same time, the business culture pressure cannot be disregarded, that is if there is a wish to cooperate with esteemed credit and payment institutions, the market participant needs to have money laundering and terrorist financing internal rules and control mechanisms set.

Positive aspect is that all respondents have appointed a responsible employee or employees to work on ML and TF prevention. Only 14.3% of respondents confirmed that ML prevention is their only task, the rest (85.7% of respondents) perform other tasks as well as responsible persons. The aforementioned indicates vulnerability – the market participants are not ready to contribute and invest into ML prevention by hiring the necessary people. Since ML prevention in the sector of finance is so to say a matter of hygiene, vulnerability would be greatly reduced if a specific person was appointed for the task who can work on ML prevention without being influenced by business decisions.

The survey results indicated that 21.43% of crowdfunding service providers have been in a situation where the investor has prohibited submitting additional information on financing sources to the company and observed thus hiding of beneficial owners. 14.29% of the respondents have identified that financing projects with no reasonable economic basis have been submitted to them. 7.1% of respondents have noticed in their activities underlying transactions with criminal background and ill-intentioned behaviour by the project owners who want to commit investment fraud.

64.3% of market participants cannot assess the pressuring methods of foreign supervisory authorities in terms of breaching ML prevention requirements. The aforementioned indicates that there has been no contact and therefore sector vulnerability in this domain is low. The company employees' understanding of the obligation to report suspicious transactions is present for 85.7% of respondents and on good level. This is very positive and there is no vulnerability. 71.4% of respondents confirm that the company assesses compliance control sufficiency regularly. This is positive and there is no vulnerability. Almost half of the respondents (42.9%) assess the sufficiency of compliance control more frequently than once a year and 28.6% assess it annually. This indicates that market participants take ML prevention seriously which also reduces vulnerability. Survey respondents disclosed that they last assessed compliance control sufficiency 4-6 months ago (35.7% of respondents), 2-3 months ago (14.3% respondents) and one month or week ago (both 7.1% of respondents).

A half (50%) of the respondents use risk-based approach in identifying financial crimes. The rest either do not have it or they do not know how to comment. The aforementioned indicates that market participants do not have sufficient knowledge of risk-based approach and this definitely increases sector's vulnerability. The main system used for identifying financial crimes is monitoring transactions and client's activities (44.4%).

71.5% of respondents have a system for monitoring suspicious activities, covering a capacity for identifying suspected ML transactions in 42.9%, capacity for identifying suspected TF transactions in 35.7% and capacity for identifying suspected financial sanctions transactions in 64.3%. The existence of a system significantly reduces sector's vulnerability to committing ML and TF. A system for monitoring suspicious transactions involves different activities and is not limited only with doing a background check, for example, one system for market participant monitoring is manual and individual for each transaction. 26.7% of respondents had automatic control, 33.3% perform background checks (sanctions list, PEP register, etc.), in case of 13.3% the system alerts a suspicious transaction and 20% observe transaction limits. The variety in procedures is positive and reduces vulnerability. For a half of the respondents (50%) the transaction monitoring system is semi-automatic.

78.6% of respondents adhere to the risks identified with IT solutions in monitoring scenarios. This percentage is high, and it is positive that market participants mainly approach ML prevention risk-based. There is a certain vulnerability in that each market participant does no know what their areas' risks are and how to monitor according to the risks related to their company.

The frequency with which the risks identified with monitoring scenarios are reviewed and adjusted, are very different starting with "all the time" and ending with "once a year". The companies reviewed the risks used in monitoring scenarios most often (21.4%) the last time 2-3 months ago, but here too the answers vary, and common conclusions cannot be drawn.

A company's business relations transaction monitoring system allows identifying complex or unusual transactions for 50% of respondents, the rest do not know or do not have the system with such capacity. For 42.9% of companies whose business relations transaction monitoring system allows identifying complex transactions, the business relations monitoring system also adheres to client profile when identifying unusual transactions (question 64). The fact that in majority the identification of unusual transactions by system depends on the client profile is an important indicator which allows better distinction of unusual transactions because the unusual transaction structure is directly related

with the client's own profile. Depending on the client, the unusual transaction may not be so to say unusual. For 42.6% of companies the business relations monitoring system is based on sum-based approach and client's behaviour that is different from normal. Other bases for determining were marked only by one market participant. This indicates high vulnerability because business relations monitoring system should include other analysed factors than just sum based approach and different client behaviours to effectively prevent ML.

42.9% of the respondents allows automatic client risk level calculation. The market participants' systems allowing automatic client risk level calculation are the following: a risk is calculated based on data available on the client in the system (2 companies), KYC system (2 companies), service provided by third party is used (1 company), system considers client's risk, geographical risk and transaction risk (1 company).

Only 21.4% of the respondents make regular IT audits for the transaction monitoring automatic systems of the AML programme. Indicates some vulnerability, but at the same time does not mean that the processes are not working due to this. IT audit means that the correctness of risk analysis is checked.

71.4% of market participants invest into technical risk management solutions. This is positive and reduces sector vulnerability. These investments mean the following: investments into IT solutions (23.1%), security measures are implemented (7.8%), automatic monitoring systems are used (15.4%), paid databases are used (7.8%), programmes and software is used (30.8%), digital face and document recognition system is installed (7.8%). All these investments are reasonable and necessary. The survey indicated that different solutions are used which is definitely a positive aspect in preventing money laundering.

For identifying PEPs, the paid programmes/sources available online are used the most (41.1%). Companies also use recommendations on the PBGB website for searching for PEPs, third parties, web search, interview with the candidate/questionnaire and https://namescan.io/FreePEPCheck.aspx website. For 85.7% the aforementioned sources are sufficient for identifying PEPs. One respondent finds that these are not sufficient for identifying PEPs because they do not provide all information.

50% of market participants do not know if the mechanism for reporting suspicious transactions to the FIU is user-friendly. One respondent finds that it is not user-friendly because it is too time-consuming. None of the respondents have faced problems so difficult that the report has been left unsubmitted or they were not sure. None of the respondents have received feedback from the FIU on the quality of suspicious transaction reports or they were not sure.

Vulnerabilities related to crowdfunding service providers compliance control have been assessed as average/high:

- efficiency of compliance ensuring systems – average/high,
- efficiency of monitoring suspicious activity and reporting it – average/high.

Quality of the due diligence measures framework applied to client

Virtual currency sector

The survey studied whether access to information on beneficial owners is easy. 64% of respondents find that access is easy. At the same time, two service providers have highlighted the problem that information is paid, and 4 service providers find that the information is unreliable. Also, the free of charge access mechanism of commercial register beneficial owners may contradict subsection 78 3) of the MLTFPA, because the obliged entity has the right to access only 10 legal persons' data per day; also, the commercial register does not check if the person using the free of charge access is indeed an obliged entity, which is why this system should be changed. This aspect should be investigated more deeply in the future.

According to the FIU's virtual currency service providers survey, only 0.15% of the client portfolio among Estonian virtual currency service providers' is Estonians. Since the previous statistics is estimated, this number might be even lower. Since virtual currencies are cross-border in nature, secure national identification system by identification documents issued by state is not ensured for all clients.

The FIU website presents an incomplete recommendation for conducting a PEP search.[79] The survey results indicate that only 36 service providers find that access to PEP lists is easy. As many as 9 service providers consider information difficult to obtain. The former refers to the fact that entrepreneurs check insufficiently or not at all if a person is a PEP.

In the survey, access to information that is necessary for identifying and checking foreign PEPs was also assessed. According to 22 respondents, access to data is easy and nearly half the respondents find that data exists, but access is complicated. Pursuant to the aforementioned, there is the risk that service providers do not apply the proper measures and identify foreign PEPs.

MLTFPA provides circumstances with greater risk and in cases provided in the law, enhanced due diligence measures must be implemented. 20% of the survey respondents did know which due diligence measures are used in case of instances with higher risk, which may point to the fact that the service providers have not determined the said due diligence measures or that risks related with clients are not assessed with sufficient diligence. If the entrepreneur does not determine risks related to clients and high-risk clients, it is not possible to properly implement the due diligence measures. As a result, the transactions cannot be monitored properly because the companies do not know their client or their area of activity or possible transaction volumes and/or partners. All this in turn leads to a situation where suspicious transactions are not identified or reported to the FIU.

Since according to the existing statistics, only 0.15% of virtual currency sector clients are Estonians and 1/3 of clients are from a higher-risk third countries and the legislator or the supervisory authority, excl. Financial Supervision Authority under whose supervision the virtual currency sector is not yet, have not explained how to implement the two source identification method provided in § 21, subsection 4 of the MLTFPA in practice, it may be stated that the level of due diligence measures, incl. primary identification, implemented for clients is low.

Vulnerabilities related to due diligence measures the virtual currency service providers implement for clients have been assessed as average or high:

- the existence of system that allows for risk-based calculation of a client's risk level – high,
- the efficiency of identifying a PEP – average/high.

Crowdfunding sector

Here, it is important to consider that the majority of crowdfunding service providers are not obliged entities in the sense of MLTFPA.

The efficiency of due diligence measures implemented for the client cannot be assessed at this time, because the service providers do not have regulative obligation. At the same time, the business culture pressure cannot be disregarded, that is if there is a wish to cooperate with esteemed credit and payment institutions, the market participant needs to have money laundering and terrorist financing internal rules and control mechanisms set. 71.4% of the survey respondents have developed a process how to identify beneficial owners.

Only 18.8% of survey respondents did not use measures to ensure independence of employees responsible for ML prevention when performing work tasks. Others who take care of training their employees, use various measures, most often trainings, systems where salary does not depend on performance and whistle blowing systems. Vulnerability in terms of the aforementioned can be considered low.

[79] See https://fiu.ee/kasulik-info/kasulik-info.

71% of respondents did not participate in the FIU/ISS training. This does not mean that no one participates in the trainings, but rather that information on the FIU/ISS trainings may not have reached the market participants. More than a half of the respondents are not confirmed that the information on beneficial owners in the Estonian commercial register is reliable. That is, the data in the national register is rather not trustworthy (which in itself is not a vulnerability but indicates distrust). Also, more than a half of the respondents do not have a stance on if the information necessary for identifying and checking high-risk clients is easily accessible (i.e. the market participants could not give an assessment).

Vulnerabilities related to due diligence measures the crowdfunding service providers implement for clients have been assessed as average/high:

- the existence of system that allows for risk-based calculation of a client's risk level – average/high,
- the efficiency of identifying PEP – average/high.

7.4.4. Assessment of sectoral risks with sectoral control quality

Virtual currency sector

The fact that companies operate internationally makes using these companies for ML purposes considerably easier. Since the companies do not have offices in every country to identify persons (differently from banks), but identifying is done via internet, the threat of using figureheads or stolen identities is remarkably higher.

By assessments, it does not seem like the companies would consider the topic too important. On the one hand, it seems like interest in the topic is low, at the same time it is informed that the topic is being handled, but there is nothing to report (nearly 15% have submitted reports to the FIU). Nearly 50% of the companies deem the sanctions for not complying with the requirements too strict, at the same time, no one has been punished.

Only 16 respondents conduct employee activity supervision according to their own words and carry out the control over them, which again is a sign indicating that on the one hand, the topic is not considered too important, and on the other, the risk that employees can be influenced not to report suspicious transactions increases. At the same time, this contradicts with response no. 45 where 54 companies say that there is control over performing transactions/tasks. Also, nearly 40% of companies either have not responded or do not use measures to ensure employee's independence. It is also interesting that if nearly 50% of companies use training and virtual seminars for raising the employees' awareness, then only about 10% of companies test their employees' knowledge.

Only 40% of companies use automatic risk level assessment of a client, from whom a very small number consider the client's digital behaviour.

Nearly 40% of respondents find that the mechanism for reporting a suspicious activity to the FIU is not user-friendly or they do not comment. Pursuant to this, there is the risk that the companies do not submit reports because the reporting form seems too complicated or time-consuming. At the same time, there is a small percentage of those who would want to integrate the reporting mechanism with their own platform.

The companies are mostly small with 1-5 employees and at the same time almost 50% of them inform that more than 50% of the employees work with ML and TF prevention. Even if the numbers are correct, this still means about 1-2 persons per each company who work on this topic, and according to question no. 50, nearly 65% also perform other tasks. Considering that cryptocurrency is a very attractive instrument for committing money laundering, this resource seems insufficient. Also, nearly 50% of the companies inform that they have not experienced instances where they need to use the

guide on how to inform of suspicious activity, but it seems unrealistic that 100% of transactions have been not suspicious.

Nearly 50% of companies have participated in ML and TF prevention roundtables. The rest either have not been included or they have no interest in participating. In both cases it is a weakness that makes half the companies more susceptible for money laundering.

30 respondents have indicated that they do not have systems that would be capable of identifying money coming from mixers. Additionally, 22 also responded that they do not know. Considering that cryptocurrency mixers are currently one of the most efficient measures for hiding the actual owner of the money, this indicates that the risk that such services will be used increasingly for money laundering is quite high. Additionally – the criminals can also quite easily check if such a system exists or not risk-free, because you can also use the mixer to transfer perfectly legal funds to your account. Thus, lack of such a system certainly provides a heightened risk of ending up in a money laundering chain.

According to their own words, only 9 respondents have cooperated with law enforcement in observing the dark web and just 15 respondents have informed the FIU or another competent authority, regardless that there are considerably more reported suspicious indicators – only 29 companies responded that they have "never seen any aforementioned instances". Thus, the reporting level is approximately 20% which is clearly too low. The threat here is that even if the virtual currency account is closed, if this information does not reach the law enforcement authorities, the criminals will simply pick another platform and continue their activities. By informing a law enforcement authority there is at least some probability that the persons are identified.

Nearly 50% of the companies have not implemented different mechanisms (e.g. avoiding sanctions, terrorist financing (that only 25%), radical movements, cashflows related with dual-use items, etc.) that could identify ML and TF considerably better. Also, about 40% of the companies responded "no" or "don't know" about documenting asset freezing procedure.

Vulnerabilities related to the efficiency of identifying sectoral risks have been assessed as average/high.

Crowdfunding sector

The quality of risk assessment of sectoral control cannot be assessed because there is no regulative obligation for sectoral control. At the same time, the business culture pressure cannot be disregarded, that is, if there is a wish to cooperate with esteemed credit and payment institutions, the market participant needs to have money laundering and terrorist financing internal rules and control mechanisms set.

Vulnerabilities related with efficiency of identifying sectoral risks has been assessed as low.

7.4.6. Quality of the responses to risks identified during previous assessments

Virtual currency sector

The objective of the Estonian national money laundering and terrorist financing risk assessment published in 2015 was to review and supplement the valid ML and TF prevention measures; to identify the risks per domains as a result of which the priorities of institutions can be specified; to map risks; to help the supervisory authorities to apply risk-based supervision more efficiently; to understand the obliged entities in risk-based implementing of due diligence measures of obligations pursuant to MLTFPA; successful passing of MONEYVAL. Aim of other financial service providers', incl. virtual currency service module was to analyse the vulnerability from products, offered services and client base.

Findings related with virtual currencies, which in the risk assessment are recognised as alternative payment means service, were the following: sector vulnerability assessment on a scale 0-1 is on average low, vulnerability rate is 0.2. Level of regulations was assessed high, sufficiency of reporting activity and supervision as average. The risk assessment highlights that with the new MLTFPA regulation enforced in 2008, this sector was regulated and subsequently the major risks disappeared and the interest of money launderers subsided. At the time of preparing the risk assessment 16 companies owned the alternative payment means service activity license and only 7 companies are analysed in the assessment. Pursuant to the aforementioned it is impossible to adhere to the previous risk assessment results because the number of service providers has increased significantly over the past years and thus the risks and vulnerability rate have also changed. As a result of the risk assessment, a proposal to preserve the situation and raise the representatives' awareness through training was made to improve reporting activity.

The FIU 2018 yearbook presented as the main virtual currency service providers risks:

- frauds and asset appropriation, because owning an activity license increases reliability;
- provision of services in other countries that require financial supervision authority licenses;
- money laundering;
- terrorist financing;
- insufficient implementation of due diligence measures by the service providers which is used by criminals for moving proceeds of crime.

Also, foreign persons with suspected terrorist background have tried to open accounts with service providers that hold the FIU activity licenses. In the yearbook, it was found that the FIU's competence is not sufficient to mitigate the risks accompanying virtual currencies. The FIU made proposals to enhance the regulations, incl. license proceeding conditions. The respective amendments were enforced in the MLTFPA on 10.03.2020. To mitigate the risks, respective regulations are needed where technological development and interests of the persons using the services are also considered. Also, it is necessary to increase strategic analysis capacity to understand the risks and use the resources efficiently.

SNRA (2017/2019) found for this sector that across Europe, the ML and TF risk of virtual currency is high/very high.[80] It was proposed to the member states that heightened attention should be paid to virtual currency service providers. Competent authorities need to monitor virtual asset domains, incl. virtual currency with great attention and assess if national regulation needs to be amended. In Estonia, it is necessary to mention here that the legal framework related with virtual currency service providers has been constantly enhanced and the plan is to continue with enhancing the sectoral requirements also in the future.[81]

Below follows what was written in the analysis of the European Commission's supranational ML and TF risk assessment report (SNRA) 2017 and 2019 on virtual assets, incl. currencies.

AMLD5 handles virtual currency[82] which is a narrower term than the virtual asset[83] term the FATF uses. SRNA 2019 handles both simultaneously. AMLD5 handles virtual currency exchange for money service providers and virtual currency wallet service providers (i.e. service providers related with virtual assets are left out). Virtual currencies service providers continue to receive heightened attention, to which the Commission suggest focussing (especially transaction speed and anonymity).

[80] European Commission supranational ML and TF risk assessment report (SNRA) 2017 and 2019 analysis.

[81] Draft legislation on crowdfunding and other investment instruments and virtual currencies, see text in legal framework chapter.

[82] *Virtual Currency – A digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically.*

[83] FATF – Virtual Asset – *A digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*

In the said domain the risk of ML and TF is increasing (growing number of suspicious transactions with virtual asset, incl. virtual currency). The Commission conducts an assessment on how to correctly regulate virtual assets, incl. virtual currency service providers in terms of implementing ML and TF prevention due diligence measures (incl. risk analysis, cooperation with member states, etc.).

According to the SNRA, sector vulnerability in terms of ML is considered high or very high and factors referring to ML threat are:

1. anonymous and fast transactions (without identifying the owner);
2. using internet, i.e. cross-border risk that allows making transactions with high-risk clients or clients from high-risk regions who cannot be identified;
3. decentralised service provision channels (incl. ATMs);
4. rapidly developing technology, with which risk awareness is difficult to keep up;
5. financial intelligence units do not have access to identifying the origin of e-wallets and funds;
6. lack of wider regulation (which would also cover virtual assets more widely).

Crowdfunding sector

This is a new sector that is gaining popularity. Thus, crowdfunding sector was not covered in the previous NRA. This sector was not assessed in the NRA 2015.

SNRA (2017/2019) found for this sector that across Europe, the ML and TF risk of crowdfunding is on average high.[84] Criminals may use the platform to raise funds (gathering funds from legal or criminal activities using anonymous products) and send these abroad with the aim of money laundering or terrorist financing. Rather the crowdfunding sector has been used for fraud (e.g. complex Ponzi schemes – frauds and fake projects) for laundering illegal funds. The following proposal was made to the member states: if the member state adopts AMLD 4 and 5, then the member state must consider the need to handle the unregulated crowdfunding platforms as obliged entities in terms of the AML/CFT regulation. In Estonia, currently the draft of ACOIIVC regulation is being proceeded, the aim of which is to regulate the Estonian crowdfunding sector. With the aforementioned draft act, the aim is to add the crowdfunding service providers as MLTFPA obliged entities. According to explanation point 32 of the EU crowdfunding regulation which is implemented from 10.11.2021, the European Commission shall assess whether the entrepreneurs within the scope of the referred regulation should be obliged entities in terms of AMLD (the timeframe of the assessment is not known).

Below follows what is written in the analysis of the European Commission's supranational ML and TF risk assessment report (SNRA) 2017 and 2019 on crowdfunding. **The vulnerability of the crowdfunding sector in terms of money laundering is assessed on average as high, whereas aspects referring to a ML threat are:**

1. In case of credit and equity crowdfunding it is possible to raise larger sums (risk is higher than with donation-based crowdfunding), although in general such platforms are regulated (incl. disclosure requirements and using credit institutions);
2. virtual currency use and anonymous transactions;
3. risk of platforms created by organised crime;
4. little knowledge of the origin of raised funds, extent of crowdfunding and its aim;
5. crowdfunding service providers are in general not obliged entities in terms of MLTFPA;
6. all crowdfunding business models are not regulated in the EU members states (in some states only some categories);
7. crowdfunding platforms do not operate in the country where they are registered;
8. no supervision.

[84] European Commission supranational ML and TF risk assessment report (SNRA) 2017 and 2019 analysis.

7.4.7. Conclusion

Virtual currency sector

As a result of the survey and working group discussions, the virtual currency sector vulnerability in terms of money laundering is high. However, the following factors reduce the vulnerability of virtual currency sector:

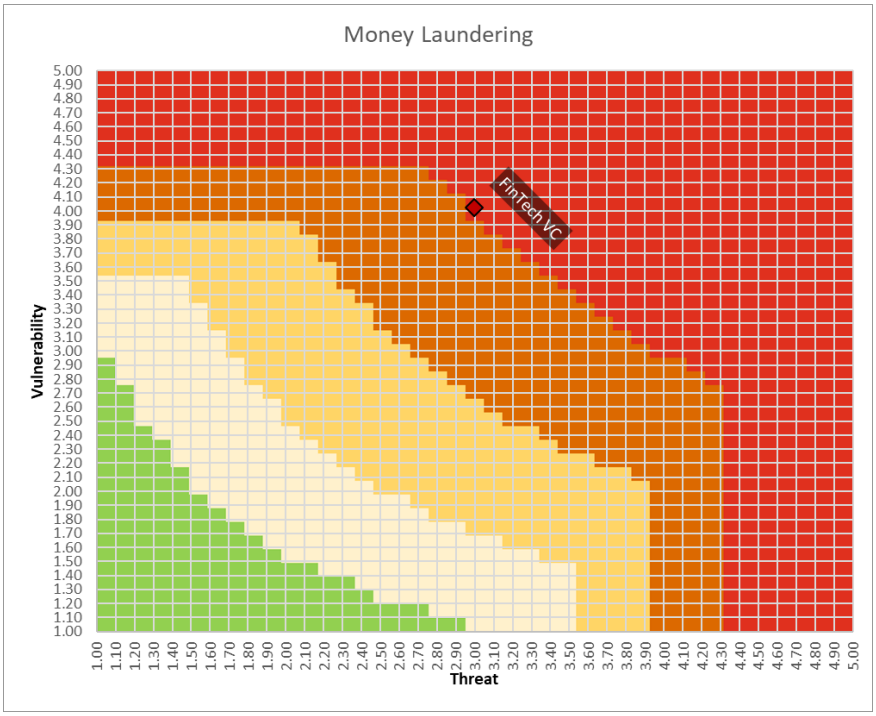
- From 10.03.2020, significant changes were enforced in the MLTFPA, as a result of which the virtual currency service providers regulation became significantly stricter, incl. stricter requirements were set for service providers which the entrepreneurs owning an activity license had to comply with at the latest by 01.07.2020. As a result of this the number of service providers reduced significantly in Estonia.
- Compared to many other EU member states, the Estonian MLTFPA regulation is of a good level. Also, Estonia was one of the first European countries where activity license obligation was enforced for providing virtual currency services.
- If the entrepreneur has not started providing virtual currency services six months after the respective activity license is issued, the FIU revokes the company's activity licence (§ 75, clause 3 of the MLTFPA.
- Respective national regulation is currently planned.

The working group also identified that the following circumstances increase the vulnerability of the virtual currency sector:

- Since the amendments to the MLTFPA took effect only on 10.03.2020, it is a new legislative framework and therefore its efficiency might not meet the presumed efficiency, and the more specific impact of the regulation amendment will be clear in the future.
- Although one circumstance of the object of control provided in section 72 of the MLTFPA is that the management board must reside in Estonia, the domain is global and therefore some service providers may still be located abroad.
- The extent of supervision and local controls conducted does not meet the size of the virtual currency sector. This is caused by the insufficient supervisory resources.
  There is a shortage of:
  a) people (in total 9 people work with the FIU supervision and issuing activity licenses. There are more than 2000 obliged entities whose existence is known thanks to activity license obligation, plus persons subject to supervision once conditions are met and persons regarding whom the FIU is unaware if they need an activity license);
  b) continued raising of their awareness;
  c) gathering of information necessary for prevention and forwarding the gained information to obliged entities and the public.
- The FIU does not have the financial resources to raise their IT capability and change the reporting form to meet the characteristics of the sector. There are also no resources to buy the appropriate programmes, to effectively analyse the obtained information and to identify with in-depth analyses the need for submitting the necessary information to law enforcement authorities.
- A lack of information on beneficial owners and complexity of checking this information gives the service consumers a chance to cover or hide the beneficial owner and origin of the asset.
- Estonian virtual currency service providers are involved in various stages of money laundering (placement, layering, integration). It is known that virtual currency service companies with activity licenses issued in Estonia are used for committing (investment) frauds abroad, for converting proceeds of fraud into virtual currencies, for operating cash ATMs without proper identification. All of them use the FIU activity licence as a legitimacy enhancing circumstance. At the same time, a licence issued in Estonia does not grant the right to operate as an investment service provider or operate outside of Estonia. Until March 2020, it was not properly possible to check those wanting to enter the market either. The existing measures also need constant upgrading to comply with the sector's developments.

- National information exchange between law enforcement authorities and the FIU concerning crimes committed regarding virtual currencies is not automatic but takes place within a specific proceeding. Thus, it is impossible to generalise the transaction patters, manners of functioning or related persons of crimes committed or suspicious activities related to virtual currency service providers in Estonia. This also reduces the FIU's capability to describe the trends related with the domain and the region and to prepare instructions for virtual currency sector.
- It is difficult to include companies established in Estonia that possess activity licenses in a criminal procedure because the victims are often located outside of Estonia, the funds may not move through settlement accounts opened in Estonian credit institutions and the persons do not operate in Estonia.

Figure 8. Heat map of the ML risk level of the FinTech VC subsector



Summary

Virtual currencies sector is a sector with **high** risk level in terms of ML. Enhanced due diligence measures must be implemented in the sector.

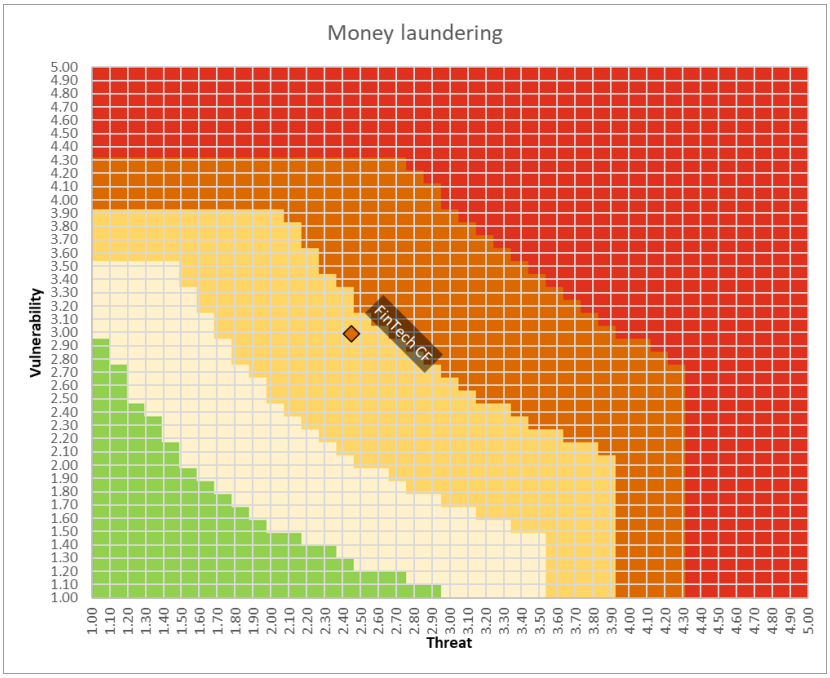
Crowdfunding sector

The assessment on the vulnerability of the crowdfunding sector is slightly above average in the ML aspect.

The strengths of the sector are self-regulation of service providers, presence of an umbrella organisation, availability of good practice and the "good practice" label awarded for successful following of the guide, good contact and communication with the public authorities and willingness to cooperate.

Other vulnerable aspects are lack or regulation and supervision, which will be solved in 2021, though. Another weakness is an access to international information on beneficial owners and PEPs, additionally correctness and accuracy of the information in the commercial register has been mentioned. This aspect needs to be solved on national level.

Figure 9. Heat map of the ML risk level of the FinTech CF subsector



Summary

In case of crowdfunding, ML risk level of the sector is rather **average**. Regular due diligence measures must be implemented in the sector.

7.4.8. Risk mitigation strategy

7.4.8.1. Risk mitigation measures at the national level

Virtual currency sector

The following national level proposals are made to improve the situation:

- Implementation of enhanced due diligence measures in the virtual currencies sector.
- Although the provisions of the 5th AML directive can be considered the first step in regulating the virtual currency wallet service and exchange for money service, the increasing use of these instruments creates a higher risk and additional regulative measures may prove necessary. In the finance sector, one of the general proposals made to the member states in terms of supervision is the recommendation to continue local checks according to identified risks, among else, these checks should focus on a specific product or weaknesses characteristic of the service.
- Improvement of international cooperation in terms of supervision because virtual currency service providers are generally active in more than one country.
- It is extremely important to harmonise the legal framework applicable to virtual currency service providers, at least at the EU level so that fair competition is ensured for the obliged entities, that risks across EU are proportionally mitigated and that the clients could not simply ignore the due diligence measures of an obliged entity by immediately creating a new account with another service provider when due diligence measures are implemented.
- One mitigating measure on national level is increasing the resources of competent authorities (the FIU and/or the FSA)[85] to conduct supervision, since the volume of supervisory activities

[85] The competent authority or division of competences may change in the future. See also proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, available at: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

and on-site checks does not currently comply with the size of the virtual currency sector, also publishing more instruction materials and ensure information exchange and regular communication with market participants.

- Also, service provider's activity requirements must be enhanced for virtual currency service providers and a reporting obligation must be imposed. Precise statistics will provide a better overview of the sector in the future and allow for more deliberated policy decisions as well as more efficient assessment of risks related to service provision. In terms of the reporting obligation, a need is seen in the future to obligate the virtual currency service provider to ask the client to give additional personal information, e.g. the first name and last name or names; the place and time of birth; the citizenship or citizenships; the gender, the number and a copy of the identification document; the telephone number and e-mail address.
- The FIU's training for the sector to identify mixer transactions and for implementing necessary methods and solutions.
- The FIU's feedback to virtual currency service providers revealed that less than 5% of entrepreneurs submitted reports to the FIU in 2019[86]. This may refer to the fact that the measures implemented by the supervisory authority if the reporting obligation is not performed are inefficient, thus this aspect needs to be analysed more deeply in the future (i.e. thorough analysis/supervision concerning report submission should be carried out). A mitigating measure at the national level could be the establishment of administrative fine proceedings.
- Based on the information obtained from the reports submitted, the FIU can obtain an overview of the sector's risks and understand the vulnerabilities. Accordingly, there is one mitigating measure to make the FIU's online reporting form more suitable for the domain of virtual currency service providers. To this end, input from the market participants could be used, that is, what data they think need to be added to the reporting form to make the submission of reports as convenient as possible and to avoid a situation where the service provider fails to submit a report due to the reporting form's complexity.
- To give the reporting sectors feedback on issues related with suspicious reports.
- In September 2020, the Estonian FIU published the results of the survey of virtual currency service providers, for which questionnaires were given to all companies at the end of 2019 who had been issued an activity licence based on data in the register of economic activities either for exchanging virtual currency for money and/or a virtual currency wallet service before 30 June 2019. The survey also presented an overview of the turnover of the transactions and customer base. In order to draw adequate conclusions on the sector also in the future and to identify the accompanying risks, data on market volumes and turnover should be published regularly. The FIU also highlights in the survey that a reporting obligation should be enforced for the service providers for transactions, clients and volumes, which would provide a comprehensive overview of the sector.
- The obligation to create the function of a Money-Laundering Reporting Officer (MLRO) or to create a respective position, incl. the fit & proper criteria required from this person, would lower the risk of the entire sector, market participants and their client portfolio as well as raise the management's awareness and commitment, the result of which could be increasing investments into compliance control systems and due diligence framework.
- A register or a data exchange portal should be kept that includes correct and updated information on beneficial owners. Supervisory authorities or other law enforcement authorities must also have access to this information. The company and shareholders must have an overview of who are their beneficial owners and this information must be available to law enforcement or supervisory authorities at any time.
- Already existing information (i.e. financial data, business, real estate, registered immovables and other registries, tax information, stock exchange information, etc.) must be used for enriching the data.

[86] According to the FIU's information, the number of entrepreneurs submitting reports increased nearly three times in 2020.

- A payment account must also be opened when establishing a company. Accordingly, there will automatically be a person who has access to this account and this information can be used as one source for assessing the beneficial owners.
- Indicators that allow identifying risky companies should be defined. This would allow creating a red flag system that could automatically identify companies with unusual behaviour. After that, manual control can be used.
- Cooperation between supervisory and law enforcement institutions should be enhanced.
- The FIU's intervention/supervision must be enhanced. More on-site controls should also be conducted. Thus, additional resources should be provided to the FIU. European Commission also stresses in the 2017 risk assessment the need for increasing the number of on-site supervisory checks. According to the risk assessment, the supervisory authority must enforce a risk-based supervision model.[87] According to the guidelines from the European Supervisory Authorities (ESA)[88] the supervisory authorities should check periodically and *ad hoc* if their risk-based supervision model is giving the desired result and if the resource level allocated for supervision is in proportion to the identified ML and TF risks. Therefore, according to the Commission, it is important that the supervisory authorities conduct sufficient on-site checks that are be proportional to the identified ML and TF risks.[89] The number of on-site checks in the virtual currency sector compared to the number of service providers is marginal.
- Cooperation between supervisory or law enforcement authorities and service providers should be improved. According to the Commission risk assessment 2017, the competent authorities and obliged entities should regularly cooperate, which would also help to identify suspicious transactions more easily. Supervisory authorities should issue initial clear instructions about risks and due diligence measures related to ML and TF prevention, but also on how to identify the most significant indicators of ML and TF. In the 2019 risk assessment, the Commission also calls on the member states to enhance cooperation between competent authorities and obliged entities.[90]
- Clear countermeasures to illegal activities should be imposed. Matters related to criminal proceedings, e.g. obtaining and receiving evidence, should be clearly regulated. It is also necessary to ensure that the legislation includes the respective procedural bases. A legal analysis should be conducted, if necessary.
- Matters concerning confiscating and seizing crypto-assets should be discussed at the institutional level and respective legal measures should be planned. It should be clear when crypto-assets should be exchanged for fiat money and when they should be stored as cryptocurrency. It should also be considered what to do in a situation when a seized asset is located in a digital environment which is closed during the judicial proceedings.
- Trainings for officials and regulators (concerning both ML and TF).
- The state should also contribute more in training of the market participants.
- According to proposals of virtual currency service providers, the main thing to do for improvement of the ML and TF risk identification is to prepare clearer and more concrete instruction materials per fields of activity and practical ML training should be organised more frequently. In order to improve compliance with Estonian legislation and international standards, the service providers say it is important to raise the society's awareness, for example, by training, to ensure clearer requirements and instructions, and official, reliable and free databases for conducting background checks. Proposals for both topics primarily indicated the importance of training, which should be provided to the market participants more and which could mitigate the risks in terms of the market participants' awareness.
- Issues related to the commercial register:

[87] Commission risk assessment 2017, p 17.

[88] Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis (07.04.2017). Available at: https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20(ESAs%202016%2072).pdf.

[89] Commission risk assessment 2017, p 17–18.

[90] Commission risk assessment 2019, p 17.

- A risk may exist itself in the fact that data in the register is paid, excl. data of the beneficial owner to a minimum extent. Since it is by nature a cross-border service, it is not wise in terms of practicality or the budget to have access to all the EU commercial registers, especially when the obliged entity offers services only to physical persons.
- In a situation where the register data, especially historical information on management board members and both current and historical information on owners, is available for free to all obliged entities, the implementation of due diligence measures would be considerably easier and more affordable for the market participants and would bring the following positive effects:

Better organisation of the commercial register would ensure higher quality of implementing due diligence measures and is directly connected with a risk-based approach because it helps the obliged entity to save time and resources to work on mitigating the actual risks, i.e. customer relationships, in the case of which services are offered to non-residents, especially on, for example, Mediterranean islands. There would be less of time-consuming direct contact with Estonian clients.

This has a positive effect also in situations where the due diligence measures are implemented in direct contact with the client. Unlike banking where the wave of enhanced due diligence (EDD) rolled over in 2017, in the EU FinTech sector it is not yet as common, especially from the client's perspective and also considering the circumstance that the FinTech sector is very competitive with multiple service providers. Unlike banking where a person can have a settlement account, standing orders, a life insurance, CASCO and a home loan all with one service provider, the FinTech services are usually more concentrated, meaning it is very easy to change the service provider. Thus, when a client feels like the due diligence measures of a FinTech company are too strict and time-consuming for the client, they are happy to change the service provider, which is why the obliged entity will lose the client and will be subject to additional obligations pursuant to §§ 42 and 44 of the MLTFPA.

Additionally, the aforementioned will help the obliged entity in choosing the market, meaning that if the obliged entity finds that similar volumes can be achieved also on the Estonian market, the risks related to the cross-border aspect will also diminish. In conclusion, we find that the risks of both the FinTech sector and the financial sector as a whole could be mitigated if the commercial register data was available for free. If this is nevertheless too expensive for the state, the availability of data could be ensured until certain criteria are fulfilled, e.g. X turnover, X income or having a supervisory body.

- Before the next risk assessment, an analysis should be conducted on the financial sector, incl. to identify which service providers should be additionally assessed under the FinTech sector. The risk assessment methodology should be designed accordingly.

Crowdfunding sector

- The crowdfunding sector needs regulation and enforced supervision (the respective draft act is in process in 2021).
- The obligation to register the activity in the register of economic activities should be enforced for donations-based and rewards-based crowdfunding models. This is necessary to provide a comprehensive image of service providers and to make risk-related assessments of the sector smoother in the future.
- Crowdfunding service providers need additional measures to increase their awareness of risks as well as of internal protection measures against misuse of their services. Therefore, supervisory authorities could prepare guides or organise discussions/training (incl. for example on implementing due diligence measures, risk assessment and practical examples of the methodology that is currently used).
- Raising general awareness. People placing money via crowdfunding platforms, i.e. the investors should check the service provider/platform, the respective economic indicators, reliability of the service provider's owner/management, incl. previous projects before making

the investment. It needs to be taken into account that since currently, crowdfunding service providers are not subject to financial supervision, the requirements for the professional skills and loyalty obligations of a service provider do not apply to them.[91]

7.2.8.2. Risk mitigation measures at the level of obliged entities

Virtual currency sector

- The conducted survey indicated that from the 99 virtual currency service providers only 35% have participated in the training organised by the FIU. Since the last training for virtual currency service providers was held in autumn of 2019 and was aimed at beginners, the number if the FIU's training courses should be increased in this sector, whereas the training should be aimed at both starting entrepreneurs and those already in business. To this end, the supervisory authority needs to be ensured sufficient monetary and human resources, as well as time for training the needed personnel. The University of Tartu also organises refresher courses which are popular among virtual currency service providers.
- The obliged entities are included in the amendment of the MLTFPA through professional associations. However, the sector is seen as insufficiently involved in the discussions and law creation. Since this is a new and a small-scale domain in the Estonian financial sector, the market participants' impact is low. Therefore, obliged entities should be involved more in the discussions and regulation amendment, and information exchange between the FIU and the market participants should be enhanced. Obliged entities can also submit proposals to the FIU for making changes or point out risks, occurring problems and how the FIU can change or improve the situation.
- The cooperation between the market participants and supervision should be enhanced. The market participants are open to communication with supervisory authorities and expect the "supervisory" contact to develop into cooperation where both parties are open to information exchange, and which is based on constructive mutual education.
- According to proposals from the virtual currency service providers, the main thing to do for improvement of the ML and TF risk identification is to increase control over clients / transaction partners and to use automatic control. In order to improve compliance with Estonian legislation and international standards, the service providers say it is important to raise the society's awareness, for example, by training, to ensure clearer requirements and instructions, and official, reliable and free databases for conducting background checks. Proposals for both topics primarily indicated the importance of training, which should be provided to the market participants more and which could mitigate the risks in terms of the market participants' awareness.

Crowdfunding sector

- NPO FinanceEstonia unites Estonian crowdfunding companies; according to the latest data there are only 5 of them. Considering the fact that there are considerably more entrepreneurs active in the domain, the rest could also join this umbrella organisation. This could be used for increasing (incl. trainings) the market participants' awareness and knowledge of TF risks and implementation of the respective due diligence measures.
- Crowdfunding service providers need additional measures to increase their awareness of risks and also of their internal protection measures against misuse of services and more precise regulation is necessary.[92]
- The crowdfunding service providers should pay special attention to jurisdictions that are known for financing or supporting terrorist acts or where it is known that there operate groups who commit terrorist acts, and in jurisdictions under financial sanctions, embargos or

[91] Estonian FinTech sector vulnerabilities, document analysis.
[92] Source: https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.

measures (issued by the EU or the UN, for example) that are related to prevention of terrorism, terrorist financing or its spreading.

7.5. Vulnerabilities of prevention of terrorist financing

7.5.1. Exposure to threat

In this NRA, the **terrorist financing vulnerability level** of FinTech sector was assessed[93] as follows:

Table 40. Terrorist financing vulnerability levels of FinTech subsectors

FinTech sector	**Terrorist financing vulnerability level on sectoral level**	
Virtual currencies	**2.88**	average
Crowdfunding	**2.09**	average/low

Virtual currency sector

- Although identifying the origin and destination country is considerably easier in case of virtual currencies than in case of fiat currencies, especially cash, the sector's risk is nevertheless high.
- The client portfolios of obliged entities – according to the survey conducted in the risk assessment, slightly less than 10% of the clients of virtual currency service providers are from Venezuela, nearly 5% of the persons are from Russia and Indonesia and more than 2% of the persons are from Iran, India, etc. The risk of high-risk third countries does not involve only clients, that makes up 1/3 of the entire client portfolio, but also company owners, and it is also apparent in the fact that the majority of the companies holding the activity licence do not have any connection with Estonia.

Crowdfunding sector

- Crowdfunding is considered a terrorist financing method that is gaining popularity (especially if virtual currencies can be used as well). In practice, up till now there have been no cases where it has been identified that the Estonian crowdfunding sector has been used for financing terrorism.
- Terrorist financing vulnerability is average high because of the following vulnerabilities:
- In Estonia, the sector is largely unregulated, but the respective draft legislation is being processed in 2021. EU crowdfunding regulation was enforced on 10.11.2020 and it will be applied from 10.11.2021. The following problematic aspects are also related to the current insufficiency of the regulation, however these should be solved by the end of 2021 because of new sector-specific legislation.
- Crowdfunding platforms registered in Estonia may not factually operate in Estonia where they are registered;
- There is no supervision;
- There is no obligation to follow the MLTFPA requirements.
- There is a possibility to use virtual currency.
- There is a possibility for criminals to use an undercover agents.
- Estonia did not have a national crowdfunding risk assessment until now (exists since 2021).
- Small sums and gathering funds using keywords that refer to donations or other humanitarian support are mainly used in connection with threats, also allowing anonymity. Also, cross-border crowdfunding platforms are used, in case of them the investor might not have an actual overview and understanding of the project that is supported (incl. the option to check the information presented in the project). Considering the fact that when placing small sums into

[93] Assessments given by the NRA threats working group, which are based on the risk assessment performance method.

crowdfunding, people usually do not have specific knowledge of the field, it is also heavily managed on people's emotions of (e.g. support collected for humanitarian aid although it is unclear whether the funds collected will actually reach the alleged people in need).

- Since most crowdfunding service providers are not obliged entities in the meaning of the MLTFPA, they do not have the obligation to implement terrorist financing due diligence measures, which in turn leads to the situation where the service provider does not check who is the beneficial owner of the financed project or support. This raises the terrorist financing vulnerability.
- Cross-border nature of crowdfunding is also a significant vulnerability that adds to the situation where, for example, people from countries with higher terrorism levels raise funds through a crowdfunding service provider established and registered in Estonia. It is important to understand that it is not necessary to collect large sums to finance terrorism, small sums are enough to commit acts of terrorism.

7.5.2. Risk awareness

General risk awareness

Virtual currency sector

- Risk awareness is rather low.
- The global scale of virtual currency makes conducting supervision and investigation by law enforcement authorities difficult. Transactions are made across borders and using multiple service providers located in different jurisdictions. Thus, it is difficult to determine to which jurisdiction the performed transactions belong and how to ensure availability of the respective information. Whereas it is also possible that the transactions are not under any country's jurisdiction, which is why it is impossible to conduct any supervision.
- The Estonian Financial Intelligence Unit needs information on transactions, assets used in the transactions, wallets and beneficial owners of the transactions to obtain an overview. The risk is also higher with products that have higher limits, because it is possible to keep a large amount of virtual money on the account at once and the money can be withdrawn in cash. A vulnerability is also such virtual currency administrators who are located in countries with insufficient money laundering and terrorist financing prevention laws.
- Due to the transaction speed and the fact that virtual currency service providers are often located abroad, it is difficult for the FIU to restrict further transfers of virtual currencies and request information from the obliged entity. Additionally, the existence of an activity license (e.g. virtual currency service provider activity license) increases the trust in consumers, which allows for fraud and misappropriation of consumers' property. Also, virtual currencies regulation differs from state to state, therefore the countries do not have the same overview of the sector or the capability to carry out a control. For example, one transaction party is located in a country where the transaction participants are not identified or verified and history of transactions that would be linked with a concrete person cannot be submitted or the regulation is weak, information is unavailable for the FIU and tracing the money becomes impossible. Such virtual currency service providers also create risks who do not store private keys on behalf of the clients, but offer so-called tools that allow the client to store one's own private key and therefore the service provider may not have access to the wallet.
- A lack of legislation or its insufficiency can be considered the main vulnerability. Also there is currently no wider regulation that would regulate virtual assets in a wider sense. The MLTFPA presents a definition for virtual currency which is too narrow for newer virtual assets because the newer virtual assets do not fall under the definition provided in the law and are thus not subject to the regulation either. Using tokens is increasingly popular and these are not covered by the virtual currency definition. Ministry of Finance has submitted a draft act[94] for first round of approval, the aim of which is to regulate also such crypto assets and crypto asset service providers who are not subjected to the current MLTFPA regulation.

[94] See more: the draft legislation on crowdfunding and other investment instruments and virtual currencies.

- According to the methodology, the vulnerability related to the awareness of the service provider's employees on TF prevention was assessed as high.

Survey results of awareness:
The results of the survey conducted within the NRA indicate that the sector's awareness on TF prevention is rather modest. Reasons for that are described above.

The sector's reporting statistics is supported by the survey feedback:

- The sector performs its reporting obligation modestly. 6% of the survey respondents did not have or did not know if their company had developed a methodology and/or guide for reporting suspected TF or unusual transaction. At the same time, the service providers are obligated to enforce a methodology and instructions if suspicion of ML and TF arises or if an unusual transaction or circumstance occurs, and instructions for following the reporting obligation. The survey also revealed that more than a half of the service providers have not needed the guide in practice yet. Considering the annual turnover of the survey respondents, it is suspicious that with turnovers on these levels, the companies have not faced circumstances that should have been reported to the FIU. This hints that the service providers do not follow the reporting obligation set in the law and do not forward many important reports and suspicions to the FIU and that is why the FIU does not have the necessary information for identifying the risks and schemes spreading in the sector.
- The lack knowledge of service providers on how to implement risk-based approach to implementation of due diligence measures, which means that the service provider is not considering possible threats and implementing due diligence measures does not comply with the client's risk profile, the result of which is that the due diligence measures are implemented at a considerably lower level.
- Virtual currency service providers were asked if the sector's professional association or an umbrella organisation has developed guidelines on preventing ML and/or TF for the sector's companies. Slightly more than 40 service providers state that such guides exist and they have been of practical use for the company. At the same time, some service providers have found that the guides are insufficient in terms of ML and/or TF. Also, nearly 80 service providers say that the supervisory authority has developed guides for ML and/or TF prevention and 80 respondents find that the guides have been of practical use for the company. Since for a large number of survey respondents, the respective guides meant for service providers have been of practical use, the probability that the service providers will prevent the risks of service provision is greater, they will adjust their risk management model accordingly and submit the necessary data to the FIU. At the same time, there is the threat that the guides will not reach all service providers, because many of them did not know if such guides exist and several service providers thought such guides have not been issued.

Based on the aforementioned, the sector's general risk awareness of terrorist financing is low.

Crowdfunding sector

- The risk awareness of the crowdfunding sector can be considered average at this time. The low level of knowledge may be due to the insufficient regulation of the sector, but the EU crowdfunding regulation will be implemented from 10.11.2021 and at this time, the draft Act on Crowdfunding and Other Investment Instruments and Virtual Currencies is being processed. In relation to the aforementioned, effective investor protection is also intended to be enforced that will no doubt make the activities of entrepreneurs more transparent. Considering that the domain has also received media attention over the past years, the society's awareness of the sector is definitely on a rise. The investor-bloggers who write topics related to crowdfunding also contribute to this rise.
- There are several crowdfunding service providers active in Estonia who voluntarily comply with normal financial sector requirements and who do it already now, among else with the aim of applying for the respective activity licence in 2021 or following years for providing a crowdfunding service. Several on them also follow the crowdfunding good practice guide

prepared by NPO FinanceEstonia, which, according to the survey feedback, has been helpful for the service providers[95]. According to the survey, about a half of the respondents have found the guide useful. More than a half of the respondents have also found the FIU's instructions useful. The majority of the survey respondents have imposed internal rules according to section 14 of the MLTFPA although the law does not provide for such an obligation for them. This is likely pressure from the business culture (e.g. pressure by credit institutions).

- According to the methodology, vulnerability related to the awareness of the service provider's employees' of TF prevention was assessed as high.

Survey results of awareness:
The results of the survey conducted within the NRA indicate that the sector's awareness on TF prevention is average.

The sector's reporting statistics are supported by the survey feedback:
Understanding of the company employees of the obligation to report suspicious transactions is present in the case of 85.7% of respondents and is at a good level. This is very positive and reduces vulnerability.
50% of the market participants do not know if the mechanism for reporting suspicious transactions to the FIU is user-friendly. One respondent finds that it is not user-friendly because it is too time-consuming. None of the respondents have faced problems so difficult that the report has been left unsubmitted or were not sure. None of the respondents have received feedback from the FIU on the quality of the suspicious transaction reports or they are not sure.

Based on the aforementioned, the sector's general risk awareness of terrorist financing is average.

Commitment of management and leader role
Virtual currency sector

- The survey results indicate that risk awareness is low in the sector and needs enhancing. The results show that Estonian virtual currency service providers have had no contact with the enforcement measures of foreign authorities, thus, these rather have no impact on Estonian service providers. Although § 72, subsection 1, clause 5 of the MLTFPA provides that the virtual currency service provider must have a settlement or payment account, it is presumed that the payment account is opened with a foreign payment service provider, which raises the service provider, screening and supervision risk.
- To conclude the survey, it can be said that the comprehensiveness of the "know-your-employee" programme is rather lacking and the employers do not know their employees sufficiently, which creates a high risk.

Management commitment and leadership was assessed according to the methodology in three subclauses, the vulnerability assessments of which were the following:

- pressure from the market to follow ML prevention standards - high;
- presence and efficiency of internal control - average/low;
- honesty of employees - average.

Crowdfunding sector

- Since the market participants generally cooperate with credit institutions, some market participants implement due diligence measures provided in the MLTFPA voluntarily (due to so-called business culture). Without cooperating with a credit or payment institution it would not be possible to own an account via which one can raise money.
- The majority of the respondents conduct a background check when recruiting people, which reduces the sector's vulnerability. 35.7% of the respondents evaluate employee reliability also during the employment. The majority of the respondents provide training for their

[95] Nearly half of the respondents have considered this useful.

employees and offer thematic online courses. This indicates a good level of awareness and thanks to undergoing training, vulnerability is rather low.

Management commitment and leadership was assessed according to the methodology in three subclauses, the vulnerability assessments of which were the following:

- pressure from the market to follow ML prevention standards - average;
- presence and efficiency of internal control - average/high;
- honesty of employees - average/high.

7.5.4. Quality of discovering terrorist financing and preventing proliferation

Quality of supervision

- Developing, preparing, storing, owning, forwarding, selling or giving into use in another manner or offering a chemical, biological or bacterial weapon or another internationally prohibited weapon of mass destruction or another weapon or its significant part is already punishable (§ 98 of Penal Code).

Virtual currency sector

- Since until recently, supervision has been mostly about data enquiries and revoking activity licenses, the general due diligence and managerial commitment have been low in combatting ML and TF. Number of on-site checks compared to the number of service providers is marginal. Number of remote checks should also be increased.
- The FIU has checked on-site only 2 providers of all the virtual currency service providers that participated in the survey conducted within the risk assessment. Considering the number of survey respondents, the number of FIU's on-site checks is rather small, that is the reason why market participants may feel to a certain extent like there is no control. However, according to the MLTFPA amendment enforced on 10.03.2020, the company's place of business must be in Estonia and management must be located in Estonia, which enables conducting more on-site checks, since until now, many service providers were located abroad and conducting checks was difficult.

Vulnerabilities related to virtual currency service providers supervision have been assessed as average:

- the existence and implementation of punishment – average;
- the efficiency of supervision and practices – average.

Crowdfunding sector

- The quality of supervision cannot be assessed because there is no regulative control mechanism and competent authority. With the draft ACOIIVC, the legislator wants to appoint the Financial Supervision Authority as the competent authority to conduct supervision of crowdfunding service providers. The referred authority will start issuing activity licences and checking the service providers' compliance with the legal requirements. Crowdfunding service providers must in the future also follow the MLTFPA requirements, incl. requirements for TF prevention.

Thus, according to the methodology, the vulnerabilities related to crowdfunding service providers supervision can be considered high, but in 2021 the legal framework of the domain will change significantly.

Efficiency of compliance control systems and reporting

Virtual currency sector

See analysis on compliance control systems and efficiency of reporting in ML prevention vulnerabilities block.

Vulnerabilities related to the compliance control of virtual currency service providers in relation to TF have been assessed as average/high:

- efficiency of compliance ensuring systems – average/high;
- efficiency of monitoring suspicious activity and reporting it – high.

Crowdfunding sector

The efficiency of compliance control systems and reporting cannot be adequately assessed using the methodology in this risk assessment because there is currently no regulative obligation. At the same time, the business culture pressure cannot be disregarded, that is, if there is a wish to cooperate with esteemed credit and payment institutions, the market participant needs to have money laundering and terrorist financing internal rules and control mechanisms set. For a longer analysis on the efficiency of the compliance control systems and reporting, see the block concerning the vulnerabilities of ML prevention.

Vulnerabilities related to the compliance control of crowdfunding service providers have been assessed based on the existing data and questionnaires as average/high:

- efficiency of compliance ensuring systems – average/high;
- efficiency of monitoring suspicious activity and reporting it – average/high.

Quality of the due diligence measures framework applied to client

Virtual currency sector

The survey of virtual currency service providers indicates that the due diligence measures implemented by companies holding virtual currency activity licences are clearly insufficient. This problem was addressed to some extent by the MLTFPA amendment that took effect in March 2020, according to which companies with a virtual currency activity licence should have a place of business in Estonia. Regardless of that, it is likely that the due diligence level of the sector's companies will not rise suddenly, which is why the virtual currency sector should continue receiving heightened attention both in activity licence and supervisory procedures and from investigative authorities. Adhering to the results of the survey of virtual currency service providers, the FIU finds that the regulation concerning virtual currencies should be enhanced and the referred service providers should be subjected to reporting duty similar to financing institutions in terms of company transactions, clients and intermediated transaction volumes. Equalising with financing institutions meant stricter requirements for implementing due diligence measures for virtual currency service providers. While previously, the said entrepreneurs did not have to identify clients in the case of random transactions in sums less than 15,000 euros, now identification and data control no longer depend on the transaction value, a person must be identified in any case. All the requirements for identifying citizens from third countries were also enhanced. The law amendments took effect on 10.03.2020. Companies who already had an activity licence were obliged to make their operations compliant with the law amendment at the latest by 1.07.2020.[96] In 2021, the due diligence measures are further enhanced.

Vulnerabilities identified during the survey on the quality of the client control framework:

- Slightly more than a half of the respondents find that information in the commercial register is reliable. At the same time 30% of the respondents have answered "not sure" which means there is a threat that a large number of service providers do not use national registers for identifying the beneficial owners. On the other hand, it is possible that the service provider provides services only to physical persons and thus is not competent to assess the reliability

[96] Estonian Financial Intelligence Unit, survey of virtual currency service providers, 2020.

of the information. 4 service providers found that information in the commercial register is not reliable.

- Commercial register's practice may contradict the imperative subsection § 78, subsection 3 of the MLTFPA, because a person can access the data of only 10 businesses a day. To gain access to more data, the person needs to pay €11.50 monthly. Comments have been made regarding commercial register, that obtaining the necessary information is expensive.
- Only 36 service providers find that the access to information needed for identifying and checking national PEPs is easy, 37 cannot assess the aspect. The latter refers to the threat that entrepreneurs check insufficiently or not at all if a person is a PEP. As many as 9 service providers consider information difficult to obtain. The problem could also be that the system is not user friendly for the virtual currency service provider. In case of foreign politically exposed persons, more than half the respondents found that access to data is rather complicated. Survey responses allow presuming that since accessing information to identify foreign PEPs is either complicated or unavailable, the service providers will not implement proper measures and do not identify. The FIU's personal feedback is very welcome and a useful tool, which the market participants would like to receive more.
- The responses revealed that 20% of respondents did not know which due diligence measures are used in case of higher risk incidents. This may refer to the matter that the named due diligence measures are either undetermined in organisations or that there are problems with determining the client risk in general. If clients risks, i.e. high risk clients are not known, it is not possible to properly implement the due diligence measures. Internal procedural rules and risk appetite should also be worked on. According to the FIU virtual currency survey, only 3% of service providers implement client control measures.
- 65% of respondents assessed access to information necessary for identifying and checking other major risk clients (e.g. embassies, virtual currency service providers, entrepreneurs offering cash services, non-profit organisations, etc.) as reliable.

Problems identified in the questionnaire "Efficiency of terrorist financing identification and reporting it":

- 8% of respondents either do not check the international sanctions lists in relation to terrorist financing or do not know if these are checked. At the same time, 20% could not say how well these lists can be implemented. Thus, there could be confusion among the market participants regarding how the said lists should be implemented for preventing terrorist financing.
- Only 42 service providers have risk scenarios set of terrorist financing prevention. This is also illustrated by the fact that in 2019, only 6 reports concerning suspected terrorist financing were submitted to the FIU. This refers to the fact that the service providers do not pay sufficient attention to terrorist financing prevention. In reality, a small number of suspected terrorist financing reports is not unusual. It is extremely difficult for the market participants to identify.
- Considering the fact that in 2019, only 6 reports concerning suspected terrorist financing were submitted and none were submitted in 2018, the number of respective investigation is essentially non-existent. Data confidentiality is surely problematic in terrorist financing identification, i.e. the market participants expect more cooperation with the Security Police.
- According to 43%, the sector has a TFR guide, although 21% state that it is insufficient or non-existent. Thus, the quality of the guide is questionable. Although access to paid sources is good, the obliged entity has no way to make sure how efficient and adequate these are. The risk is also increased by the fact that persons in the risk lists usually have the same or very similar names, which makes screening very inefficient and rich in false-positives, which in turn damages the screening quality of the obliged entity.
- The following has been identified about the efficiency of identifying cash flows related to radical movements and hostile information campaigns or foreign propaganda – 8 service providers do not have respective control measures and 45 do not know, therefore, we can presume that more than half of the service providers do not have them. The former refers to

the fact that the service providers have not made the control implemented in the company compliant with the risks dominant in the sector – TF risks in this case.

- Considering TF risks during client control – turned out that as much as 47% of respondents have conducted controls related with radical movements and hostile campaigns, which is actually very positive because it is not the most common TF related risk. 87 service providers assess TF risks during client background check but based on the responses to previous questions this is contradictory and the entrepreneurs do not assess these risks sufficiently.
- Nearly 30% of respondents do not provide respective trainings to their employees. Although training obligation is there, access to TF typology is difficult to obtain and closed. Usually, training is aimed at preventing money laundering, and training on terrorist financing is less, not to mention training on non-proliferation of weapons of mass destruction.
- Existence of control measures meant for TF prevention – it was identified that in addition to 87% conducting background check, 76% of the respondents also monitor. Nearly three quarters of the respondents allegedly use respective control measures, but based on previous answers, this response is rather contradictory and does not allow drawing any conclusions.

Vulnerabilities related to the due diligence measures which the virtual currency service providers implement for clients have been assessed as average or average/high:

- existence of a system that allows client risk level risk-based calculation – high;
- efficiency of identifying a PEP – average/high.

Crowdfunding sector

Efficiency of due diligence measures implemented for the client cannot be assessed during this risk assessment, because the service providers do not have a respective regulative obligation. At the same time, the business culture pressure cannot be disregarded, that is if there is a wish to cooperate with esteemed credit and payment institutions, the market participant needs to have money laundering and terrorist financing internal rules and control mechanisms set.

Vulnerabilities identified during the survey on the quality of the client control framework:

- Reliability of the information on actual beneficiaries contained in national registers – less than half the respondents assess it as reliable and half do not know.
- Easy access to information necessary for identifying actual beneficiaries – 11 out of 14 assess that the information is easy to obtain.
- Comprehensive and reliable public information systems that help to check clients' data – half assess as thorough and reliable, half do not know.
- Easy access to information that is necessary for identifying and checking national PEPs – information is present according to the majority, but it is rather difficult to obtain. Positions exist, but it is hard to connect a person and a position (separately difficult in terms of family members and related persons of PEPs).
- Easy access to information that is necessary for identifying and checking foreign PEPs – information is present according to the majority, but it is difficult to obtain. Globally speaking, information on PEPs is available through paid service providers.
- Easy access to information necessary for identifying and checking other major risk clients (e.g. embassies, virtual currency service providers, entrepreneurs offering cash services, non-profit organisations, etc.) – access depends largely on the person's capability to invest into service provider's solutions.

Problems identified in the questionnaire "Efficiency of terrorist financing identification and reporting it":

- The efficiency of identifying cash flows related to radical movements and hostile information campaigns or foreign propaganda – out of 14, 5 implement, 5 do not know and 4 do not implement (3 do not have such clients).
- Considering TF risks in client control – 13 out of 14 implement, 1 does not know.

- Existence of control measures for TF prevention – half implement control measures aimed at TF prevention when monitoring, 5 do not know.

Vulnerabilities related to due diligence measures that crowdfunding service providers apply for heir clients have been assessed as average/high:

- existence of a system that allows client risk level risk-based calculation – average/high;
- efficiency of identifying a PEP – average/high.

Quality of identifying sector-based international sanctions

Virtual currency sector

In 2019, FATF adjusted its standards, introducing new requirements for the states to assess and mitigate risks related to virtual currencies. For this purpose, the states must license or register virtual currency service providers. The states should ensure that the service providers use all possible measures for preventing ML and TF, incl. client due diligence measures, collecting and preserving client and transaction data, reporting of suspicious transactions and making sure that the transactions comply with international sanctions. Also, service providers should be monitored and punished, if necessary, if they contradict the money laundering and terrorist financing prevention due diligence measures. It was also specified that following FATF's recommendations, virtual currencies should be handled as asset, income or another similar monetary value unit[38].[97]

Vulnerabilities identified during the survey on quality of identifying sanctions

- Nearly 80 service providers check the international sanctions lists, nearly a half of whom use registers/systems created by third parties for this purpose. Also, the monitoring system is semi-automatic for a half of the respondents. Since nearly 20 service providers do not check the lists and presumably do not own the respective system, there is a major threat that sanctioned persons use the services of these service providers. 92% of the respondents conduct these checks.
- The efficiency of mechanisms for identifying the avoidance of sanctions – only 35 service providers have such a mechanism, due to which the majority of service providers do not identify the avoidance of sanctions. There is also a risk that the sanctions check is not conducted in the course of monitoring but only when establishing business relations.
- Knowing and implementing the applicable sector-based sanctions – the responses indicate that only about a half of the market participants who responded have an overview of matters related to finance sanctions. 92% conduct respective checks. There is also a risk that the sanctions check is not conducted in the course of monitoring but only when establishing business relations.
- The efficiency of asset freezing mechanisms – the asset freezing procedure is documented only in the case of slightly more than a half of the service providers. Only 57% of the respondents had an asset freezing procedure set, which is why there is a threat that the market participants do not truly understand the purpose of the system for identifying sanctions. It can be concluded from the aforementioned that the referred mechanisms are not efficient.

Vulnerabilities related to the quality of virtual currency service providers in identifying international sanctions have been assessed as average.

Crowdfunding sector

It is difficult to establish the quality of identifying international sanctions because there is no information or cases where the FIU would have identified market participants breaching international sanctions.

[97] Estonian Financial Intelligence Unit, virtual currency service providers survey, 2020.

Vulnerabilities identified during the survey on quality of identifying sanctions:

- The efficiency of controlling the presence of sanctions – 11 out of 14 respondents check the sanctions lists, but have highlighted that due to data quality, these measures are difficult to implement. 10 service providers out of the respondents screen against the sanctions list. The respondents state that the sanctions search engines could be clearer.
- The efficiency of mechanisms for identifying the avoidance of sanctions – the majority of the respondents have not developed respective mechanisms.
- The existence of internal procedures for freezing assets – 42.9% responded "yes" to the question if the company has an asset freezing procedure. Thus, a significant part of crowdfunding service providers do not have a procedure for implementing the MLTFPA transaction prohibition when not implementing due diligence measures or in the case of suspected ML or TF or asset forwarding restrictions.

Vulnerabilities related to crowdfunding service providers' quality in identifying international sanctions have been assessed as low based on available data.

7.5.5. Assessment of sectoral risks with sectoral control quality

Virtual currency sector

- Since the companies operate internationally, using these companies for crime is considerably easier. Since the companies do not have offices in every country to identify persons (unlike banks), but identifying is done via the internet, the threat of using figureheads or stolen identities is remarkably higher. Nearly 50% of the companies have not implemented various mechanisms (e.g. avoiding sanctions, TF (only 25%), radical movements, cashflows related to dual use items, etc.), which would allow for considerably better identification of ML and TF. Also, about 40% of the companies responded "no" or "not sure" about documenting the asset freezing procedure. For more, see the respective ML subtopic on assessing sectoral risks.
- Vulnerabilities related to the efficiency of identifying sectoral risks have been assessed as average/high.

Crowdfunding sector

- Risk assessment quality of sector-based controls cannot be adequately assessed because there is no regulative obligation to control the sector. At the same time, the business culture pressure cannot be disregarded, that is if there is a wish to cooperate with esteemed credit and payment institutions, the market participants need to have money laundering and terrorist financing internal rules and control mechanisms set.
- Vulnerabilities related to efficiency of identifying sectoral risks has been assessed low.

7.5.6. Quality of the responses to risks identified during the previous assessments

Virtual currency sector

For more, see the respective ML prevention subchapter.

The objective of the Estonian national money laundering and terrorist financing risk assessment published in 2015 was to review and supplement the valid ML and TF prevention measures. The FIU 2018 yearbook presented as the main risks related to virtual currency service providers among else also terrorist financing. It has been identified that foreign persons with a suspected terrorist background have tried to open accounts with service providers that hold the FIU activity licences.

The analysis of the European Commission's supranational ML and TF risk assessment (SNRA) of 2017 and 2019 on virtual assets[98], incl. currencies (SNRA 2017/2019) identified in terms of this sector that across Europe, ML and TF risk of virtual currency is high or even very high.[99] It was proposed to the member states that heightened attention should be paid to virtual currency service providers.

SNRA 2017/2019 identified that virtual currency service providers continue to be subjected to heightened scrutiny to which the Commission suggests paying special attention (primarily transaction speed and anonymity). In the said domain the risk of ML and TF is increasing (growing number of suspicious transactions with virtual asset, incl. virtual currency).

It was found that TF risks are involved in the use of virtual assets, incl. virtual currency, which does not include any face to face meetings, which in turn allows for anonymous financing or product purchasing (cash payments or payments by third parties where the origin of the funds is not identified). Anonymous transactions are also an issue if the sender and receiver are not appropriately identified.

Persons offering virtual asset, incl. virtual currency mixing services that allow more privacy, faster transfers, lower transfer fees and smaller price fluctuations are also a significant ML and TF threat.

Virtual assets, incl. virtual currency service providers with criminals or legal persons that are incompliant with regulations, are also a challenge:

1. they use criminally obtained funds to create a virtual asset, incl. virtual currency company into which criminal proceeds can be paid in cash;
2. persons buy/sell large amounts of virtual assets, incl. virtual currency for other assets (without intermediaries) without these persons being registered as service providers (incl. they do not advertise their services);
3. payment service providers who offer virtual currency payment cards that support various virtual assets, incl. virtual currency (in general they register their activities in the "most suitable" jurisdiction).

It was also found that gathering data in a situation where the transaction is made in a country that is different from the payer's and payment receiver's location also makes the task more difficult for supervisory authority.

Thus it was assessed that in the case of virtual assets, the TF risk is high. Criminals use virtual assets, incl. virtual currency, increasingly more for terrorist financing (among else, instructions on how to use virtual assets are shared online).

In case of sectoral vulnerability, it was highlighted that TF threat is high or very high due to following reasons:

1. anonymous and fast transactions (without identifying the owner);
2. using the Internet, i.e. cross-border risk that allows making transactions with high-risk clients or clients from high-risk regions who cannot be identified;
3. the increasing popularity of virtual assets, incl. virtual currency among the criminals;
4. terrorist financing risk awareness is low in countries (regardless of the fact that AML/CFT regulations have been implemented for virtual assets, incl. virtual currency);
5. factors increasing the risk:
   5.1. no understanding or awareness, which makes it impossible to properly assess the impact;
   5.2. shortcomings in the valid regulation;
   5.3. likely use of credit and financing institutions as "intermediaries" (because of lacking proper risk assessment);

[98] FATF – Virtual Asset – *A digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*

[99] Analysis of the European Commission's supranational ML and TF risk assessment report (SNRA) 2017 and 2019.

5.4. making online transactions in the investment sector with limited client identification and verification control;

6. virtual currency term used in AMLD5 may be too narrow (compared to the virtual asset term used by FATF) and thus does not cover all fields of activity (incl. ICO providers)[100], incl.:
   6.1. wallet service providers who do not store private keys for clients but only offer tools so the client can store one's private keys;
   6.2. exchange services from virtual asset to virtual currency and vice versa;
   6.3. provision of financial services related with offering/sales of virtual assets.

Crowdfunding sector

This is a new sector that is gaining popularity. Crowdfunding sector was not tackled in the previous NRA. For more, see the respective ML prevention subchapter.

SNRA 2017/2019 found for this sector that across Europe, the ML and TF risk of crowdfunding is on average high.[101] Criminals may use the platform to raise funds (gathering funds from legal or criminal activities using anonymous products) and send these abroad with the aim of money laundering or terrorist financing. They may raise funds also using donations-based crowdfunding where sums are smaller. Terrorist financing cases have been identified where:

1. funds are raised using catch phrases such as: "support the widow, martyrs or religious groups/religious people";
2. sums are small (e.g. 10, 20, 50 dollars).

The following proposal was made to the member states: if the member state adopts AMLD 4 and 5, then the member state must consider the need to handle the unregulated crowdfunding service providers as obliged entities in terms of the AML/CFT regulation.

It was found that TF risk is on average high in case of crowdfunding sector.

Crowdfunding sector was not tackled in the previous NRA. SNRA 2017/2019 identified in terms of this sector that across Europe, the terrorist financing risk is on average high in crowdfunding, donations-based crowdfunding service providers are used for TF the most.

7.5.7. Conclusion

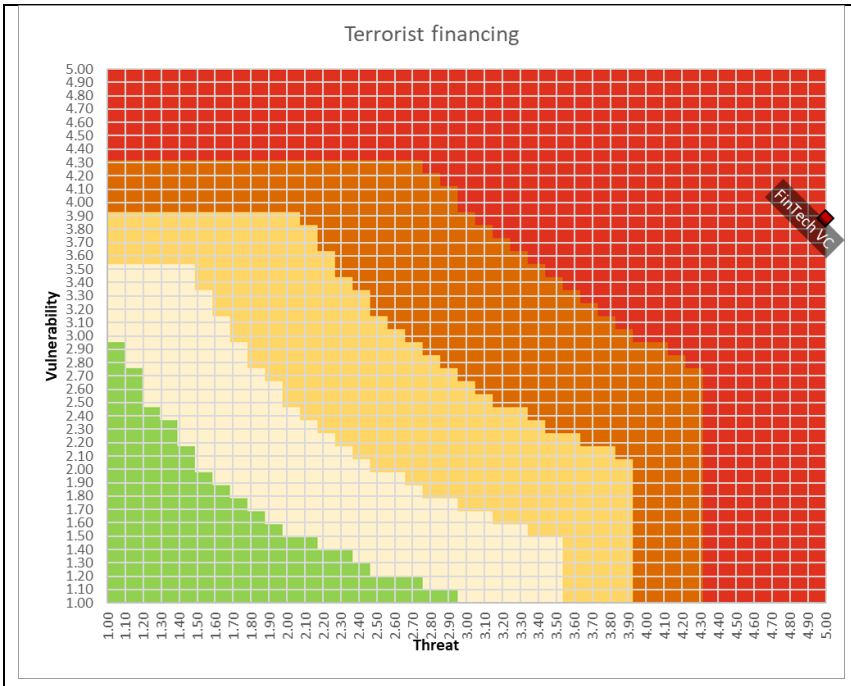
Virtual currency sector

Based on the survey and discussions of the working groups, the vulnerability of the virtual currency sector on a scale of 1-5 has been assessed as 3.88 in terms of terrorist financing, i.e. it is average. Factors reducing the vulnerability of the virtual currency sector are described in the respective subchapter on ML vulnerabilities.

Figure 10. Heat map of the terrorist financing risk level of the FinTech VC

[100] Initial coin offering (ICO).

[101] European Commission supranational ML and TF risk assessment report (SNRA) 2017 and 2019 analysis.



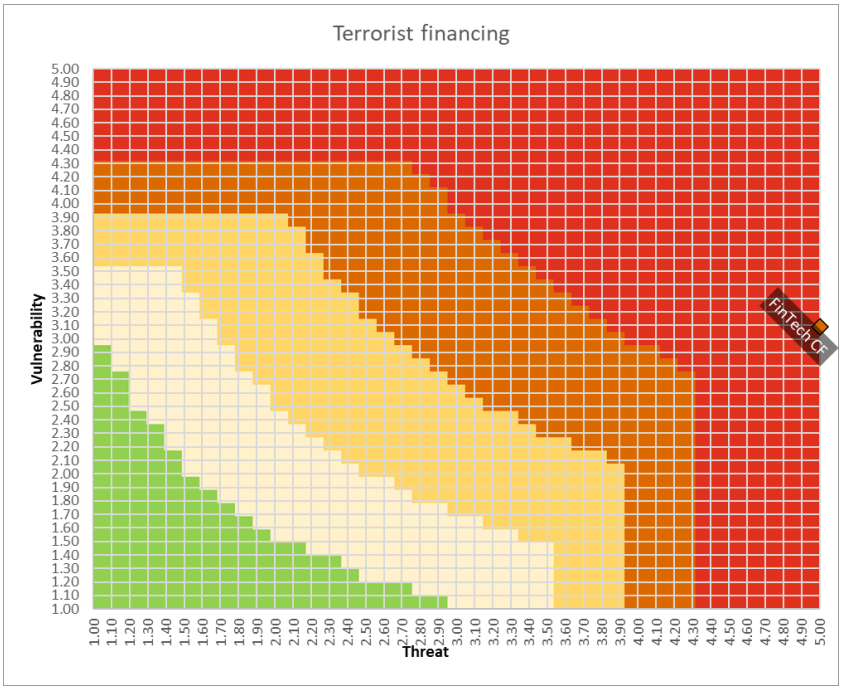
Summary

Virtual currency is a **high**-risk sector in terms of terrorist financing and this is due to the high threat. Enhanced due diligence measures must be implemented in the sector.

Crowdfunding sector

On a scale of 1-5, the crowdfunding sector vulnerability assessment in terms of TF is 3.09, i.e. it is average. Factors reducing the crowdfunding sector vulnerability are described in the respective ML vulnerabilities subchapter.

Figure 11. Heat map of the terrorist financing risk level of the FinTech CF



Summary
The risk level in terms of terrorist financing in crowdfunding sector is an **average**. Regular due diligence measures must be implemented in the sector.

7.5.8. Risk mitigation strategy

7.5.8.1. Risk mitigation measures at the national level

Mitigation measures at the national level largely overlap with what is provided in the respective subchapter on the vulnerability of ML prevention.

7.5.8.2. Risk mitigation measures at the level of obliged entities

Virtual currency sector

- A successful TF campaign requires a certain level of e-marketing, which is why identifying the respective addresses, incl. the related addresses, is up to a specialist. Since in the case of virtual currencies, identifying the origin and destination of virtual currencies is efficient by using adequate mechanisms, it is possible for the virtual currency sector, in cooperation with law enforcement authorities, incl. the Security Police, to identify the addresses related to virtual currencies that are linked to terrorist financing and clients, who are directly or indirectly otherwise related to the addresses, which in turn would allow sharing the aforementioned information with respective competent authorities.
- It is important to stress the significance of cooperation between the legislator, supervisory authority and market participants, not just via a professional association, but voluntarily between the market participants.
- To ensure greater data processing capability and quality by supervisory authorities, the FIU reporting system should be developed so as to make data about virtual currency transactions machine readable, otherwise the data processing quality is low.

Crowdfunding sector

- Crowdfunding service providers need additional measures to increase their awareness of risks and also of their internal protection measures against misuse of services and the sector needs to be regulated.
- A professional association or an umbrella organisation could be used for conducting trainings to increase the awareness of the market participants and knowledge of TF risks and implementation of respective due diligence measures.
- Such data as e-mail addresses, IP addresses and social media usernames could be added to the definitions of terrorist sanctions as information. Although respective users can easily and quickly change such identification information, adding it to the defining information would at least provide a starting point for internal investigation for companies.
- In its resolution focussed on TF, the UN Security Council invited establishing efficient partnerships with private sector, incl. FinTech sector and internet and social media companies, to fight this threat.[102]
- Crowdfunding service providers should pay special attention to jurisdictions that are known for financing or supporting terrorist acts or where groups committing terrorist acts are known to operate, and to jurisdictions on which financial sanctions, embargos or measures (issued by the EU or the UN, for example) that are related to preventing terrorism, terrorist financing or proliferation have been imposed.

[102] Source: https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.