



The Estonian national risk
assessment report in the field
of money laundering for the years
2020–2024

Contents

1. GENERAL PART	4
Introduction	4
1.1. Risk Assessment Process	4
1.2. FATF Definitions and Terms	6
1.3. Methodology Used	6
1.4. Scale and Levels of Threats	6
1.5. Scale and Levels of Vulnerabilities	7
1.6. Data Collection	8
Summary	10
Abbreviations	16
2. NATIONAL ML THREATS	17
2.1. Description of the Methodology	17
2.2. National Threats	18
2.2.1. The state of ML threats from 2020 to 2024	18
2.2.2. Sectors with a threat level above average	20
2.2.3. Provision of the ML services in organized crime	22
2.2.4. ML cases processed in 2020–2024	23
2.2.5. Trends in ML threats identified in international cooperation	28
3. NATIONAL ML VULNERABILITY	32
3.1. Description of the Methodology	32
3.2. National Vulnerabilities of the AML System	32
3.2.1. Investigation of economic crimes: resources and capabilities	33
3.2.2. Seizure and confiscation of assets	44
3.2.3. Data sources	46
3.2.4. Strategy, policy and ML crime definition	47
3.2.5. The effectiveness of domestic and international cooperation	51
4. ML VULNERABILITIES OF THE FINANCIAL SECTOR	55
4.1. Description of the Methodology	55
4.2. General Developments and Vulnerabilities of the Financial Sector	56
4.3. Credit Institutions	61
4.4. The Investment Sector	66
4.4.1. Investment firms	66
4.4.2. Fund managers and management of voluntary pension funds	69
4.5. Life Insurance Sector	72
4.6. Other Financial Services	74
4.6.1. Payment institutions and e-money institutions	74
4.6.2. Currency exchange service providers	77
4.6.3. Savings and loan associations	78
4.6.4. Credit providers and intermediaries and other financial institutions	79

5. ML VULNERABILITIES OF DNFBPs	82
5.1. Description of the Methodology	83
5.2. Gambling Organizers	84
5.3. Dealers in Precious Metals and Other Traders	87
5.3.1. Dealers in precious metals	87
5.3.2. Traders	89
5.4. Pawnshops	91
5.5. Auditors	94
5.6. Other Providers of Legal Services	99
5.7. Bailiffs and Bankruptcy Trustees	102
5.8. Accountants and Tax Advisors	107
5.9. Real Estate Brokers	111
5.10. Company Service Providers	113
5.11. Lawyers	117
5.12. Notaries	122
6. ML THREATS AND VULNERABILITIES OF VIRTUAL CURRENCY PROVIDERS	127
6.1. Description of the Methodology	128
6.2. Regulatory Changes in the VASP Sector	128
6.3. Estonia as a Transit Country for Virtual Currencies	132
6.4. Risks and Volume of the VASPs	133
6.5. Assessments	142
7. ML THREATS AND VULNERABILITIES OF LEGAL ENTITIES	143
7.1. Description of the Methodology	143
7.2. Risks of Legal Entities	144
7.3. Attractiveness of Estonian Companies	145
7.4. Threats of Money Laundering with Legal Entities in Estonia	146
8. ML RISKS OF E-RESIDENCY PROGRAM	154
8.1. Description of the Methodology	154
8.2. E-Resident’s Digital ID	154
8.3. E-Residents and Entrepreneurship	155
8.4. E-Residency Risk Management	156
8.5. Companies with E-Residents in ML Statistics	157
8.6. Trends and Summary	161
4. ANNEXES	163
Annex 1. List of Predicate Offenses for ML	163

1. General Part

Introduction

The money laundering risk assessment is part of a larger national risk assessment that includes the analysis of risks related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. The Ministry of Finance, in cooperation with the Financial Intelligence Unit, investigative and supervisory authorities, the Ministry of Justice and Digital Affairs, the Ministry of Foreign Affairs, and the Ministry of the Interior, prepared this national risk assessment, which includes the analysis of data from the years 2020-2024. More than one hundred experts from various ministries and government agencies participated in the preparation of the risk assessment, and representatives from the private sector were also involved in the process to ensure a diverse and practical perspective.

The national risk assessment (hereinafter referred to as “risk assessment” or “NRA”) is regularly prepared in Estonia every 4-5 years. The results and report of the risk assessment are published on the website of the Ministry of Finance. The results of the risk assessment are presented to authorities and market participants at information days organized by the Ministry of Finance in cooperation with the Financial Intelligence Unit and other parties, including professional associations.

To implement the risk assessment, a national risk assessment steering group, a project team led by the Ministry of Finance, and eight working groups were formed, six of which dealt with the assessment of money laundering risks. The national risk assessment report was approved by the Anti-Money Laundering and Terrorist Financing Commission under the leadership of the Minister of Finance.

The money laundering risk assessment was prepared using the methodology recognized by the World Bank¹, which was adapted to the specifics of Estonia in cooperation with the risk assessment working groups. The working groups included experts from various government agencies, representatives of professional associations, and market participants.

The Ministry of Finance expresses its gratitude to all those who contributed to the preparation of this risk assessment.

1.1. Risk Assessment Process

Money laundering is a process by which the origin of illegally obtained money is concealed, making it appear legitimate. This means that criminally obtained proceeds (e.g., from drug trafficking, corruption, tax fraud) are channeled through various transactions and channels so that the source of the proceeds is no longer identifiable.

¹ World Bank, Washington, Ameerika Ühendriigid, www.worldbank.org , see for details p. 1.3.

Money laundering generally occurs in three stages:

1. **Placement:** This is the first stage of money laundering, where an individual places the proceeds of illegal activities into the financial system.
2. **Layering:** The main objective at this stage is to obscure the connection between the criminally obtained money and its source. This is achieved through complex, multi-layered financial transactions to make tracing the transactions difficult. The money may move electronically between different accounts and countries.
3. **Integration:** This is the final stage of money laundering, where the money returns to the criminal from an apparently legitimate source, usually through banking systems. A common method is the sale of assets, resulting in the laundered money being reintegrated into the economy.

Money laundering risks were assessed from September 2024 to June 2025. Six working groups were established to assess money laundering risks.

Table 1. Composition of the NRA Working Groups for ML Risk Assessment

Assessment Area	Working Group Lead	Working Group Members
National Threats	Police and Border Guard Board	Ministry of Justice and Digital Affairs, Ministry of the Interior, FIU, Tax and Customs Board, Prosecutor's Office, Financial Supervision Authority, Internal Security Service, Environmental Board, Police and Border Guard Board.
National Vulnerabilities	Ministry of Finance	Ministry of Justice and Digital Affairs, Ministry of the Interior, FIU, Tax and Customs Board, Prosecutor's Office, Financial Supervision Authority, Internal Security Service, Environmental Board, Police and Border Guard Board.
Vulnerabilities of the financial sector	Financial Supervision Authority	Ministry of Finance, Police and Border Guard Board, FIU, Banking Union, Finance Estonia, Association of Insurance Companies, Financial Supervision Authority, representatives of market participants.
Vulnerabilities of the DNFBPs	FIU	Ministry of Finance, Ministry of Justice and Digital Affairs, FIU, Police and Border Guard Board, Tax and Customs Board, EIS, Chamber of Notaries, Bar Association, Auditors' Association, Lawyers' Union, Chamber of Real Estate Brokers, Accountants' Association, Estonian Association of Gambling Organizers, Estonian Association of Real Estate Managers, Chamber of Bailiffs and Bankruptcy Trustees, representatives of market participants.
Threats and Vulnerabilities of the VASPs	FIU	Tax and Customs Board, FIU, Prosecutor's Office, Financial Supervision Authority, Internal Security Service, Police and Border Guard Board, Web 3.
Threats and Vulnerabilities of the Legal Persons and Entities	FIU	Ministry of Justice and Digital Affairs, Ministry of the Interior, FIU, Tax and Customs Board, Police and Border Guard Board, Financial Supervision Authority, FIU, EIS.

To validate the results of the national risk assessment and evaluate the completion of the report, an NRA Steering group was formed. This group included representatives from the Ministry of Finance, the Ministry of Justice and Digital Affairs, the Ministry of the Interior, the Ministry of Foreign Affairs, the Financial Supervision Authority, the Financial Intelligence Unit, the Internal Security Service, the Police and Border Guard Board, the Tax and Customs Board, and the Prosecutor's Office.

In the first stage of the process, initial consultations were held between institutions, necessary statistics were collected, typologies were mapped, additional training sessions were conducted, and methodology experts were consulted to implement the chosen methodology. In the second stage, assessment modules were completed and analysis was conducted using both qualitative and quantitative information. Written surveys were organized, and focus group interviews were conducted. In the third stage, the report was compiled and presented to the NRA Steering group. The private sector was involved through participation in working groups, written surveys conducted during the process, and focus group interviews.

1.2. FATF Definitions and Terms

FATF defines money laundering risk as a combination of three factors:

- 1. Threat:** A person, object, or activity that has the potential to cause harm – for example, to the state, society, economy, or financial system. Examples include organized crime and money laundering schemes.
- 2. Vulnerability:** A weakness or situation that a threat can exploit or that facilitates the activity associated with the threat. Examples include inadequate supervision, weak internal control measures, lack of awareness of risks, and insufficient legislation.
- 3. Consequence:** Although not always a separately assessable component, consequence refers to the impact that threat and vulnerability together can have – for example, reputational damage to the reliability of the financial system or the economy at large.

According to FATF recommendations, countries and institutions should assess these factors to develop a risk-based approach that allows resources to be directed where the risk level is highest.

1.3. Methodology Used

The assessment of money laundering risks was carried out independently by Estonian authorities in cooperation with representatives from the private sector, using the national money laundering risk assessment methodology and tools (assessment modules) developed and provided by the World Bank. The role of the World Bank team was limited to:

1. Delivering the tool, i.e., the assessment modules;
2. Providing technical guidance on the use of the tool;
3. Reviewing the draft of the national risk assessment report and providing feedback for the accurate application of the methodology.

The data, statistics, and other information entered into the assessment modules, as well as the conclusions, interpretations, and assessments made during the national risk assessment process, belong to the participants of the Estonian national risk assessment project and do not reflect the views of the World Bank.

The World Bank's methodology guidelines and assessment modules are available to everyone on the organization's website².

As part of the cooperation between the Ministry of Finance and the World Bank, the entire team of the national risk assessment project received training and consulting services for the application and adaptation of the World Bank methodology according to the specifics of Estonia.

² <https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use>

1.4. Scale and Levels of Threats

The World Bank's money laundering risk assessment methodology uses a five-point scale to assess the levels of threats and vulnerabilities, helping to determine how susceptible a sector or system is to money laundering risks.

Threat refers to the likelihood of money laundering activities occurring. This assessment is based on the presence, origin, and extent of criminal proceeds, as well as known or potential money laundering cases. The more criminal proceeds and the more complex the money laundering schemes, the higher the threat level.

In the World Bank methodology, the final threat assessment is automatically generated after completing the assessment module, where experts evaluate various criteria such as the prevalence of crime, the size of proceeds, money laundering patterns, and related sectors. The ratings for each criterion are combined according to the internal logic of the methodology, resulting in an overall threat level for the sector or country.

1. Low Threat Level

- The volume of criminal proceeds is small or insignificant.
- Crime that could lead to money laundering is rare or well-controlled.
- There is no significant evidence of money laundering cases.
- Money laundering is very limited.

2. Below Average Threat Level

- Sources of criminal proceeds exist, but their extent is limited.
- Some money laundering cases are known, but they are not systemic.
- The threat exists but is not dominant.

3. Medium Threat Level

- Sources of criminal proceeds are significant and diverse.
- Money laundering cases occur regularly.
- The threat is substantial but not yet critical.
- It may include both domestic and cross-border sources.

4. Above Average Threat Level

- The volume of criminal proceeds is large, and money laundering cases are frequent.
- The threat is systemic and multi-layered, involving multiple sectors.
- Money laundering activities are well-organized and difficult to detect.

5. High Threat Level

- Sources of criminal proceeds are extensive and deeply rooted.
- Money laundering is widespread and complex, often involving international networks.
- The threat level is the highest possible and requires immediate and extensive intervention.

These levels help assess the extent of the money laundering threat in a country or sector, depending on the extent of crime, the origin of proceeds, and money laundering patterns.

1.5. Scale and Levels of Vulnerabilities

Vulnerability refers to how susceptible a sector or system is to money laundering, regardless of whether the threat actually materializes. This is primarily based on the strength or weakness of existing control measures, including legislation, supervision, internal controls, and risk management. The weaker or less effective these mechanisms are, the higher the level of vulnerability.

In the World Bank methodology, the final vulnerability assessment is automatically generated after completing the assessment module, where experts evaluate several criteria, such as sector risk awareness, the extent of supervision, the presence and fulfillment of reporting obligations, and other significant factors. The ratings for each criterion are combined according to the internal logic of the methodology, resulting in an overall vulnerability level for the sector or system.

1. Low Vulnerability Level

- The sector has strong and effective control measures.
- Risk prevention and detection work well.
- Supervision is appropriate and continuous.
- The system is highly resilient to money laundering risks.

2. Below Average Vulnerability Level

- Most control measures are in place and functioning, but there may be some deficiencies.
- Risk management is generally satisfactory but not fully systematic.
- Some areas need additional attention.

3. Medium Vulnerability Level

- Control measures are partially in place, but their implementation may be uneven or ineffective.
- Supervision may be limited or not sufficiently risk-based.
- The sector has a moderate risk of becoming a target for money laundering.

4. Above Average Vulnerability Level

- Control measures are weak or insufficient.
- Supervision is infrequent or formal.
- The sector is significantly vulnerable to money laundering risks, especially if the risks are high.

5. High Vulnerability Level

- Control measures are absent or non-functional.
- Supervision is non-existent or very limited.
- The sector is extremely susceptible to money laundering and may act as an amplifier of risks throughout the system.

These levels help the country and sectors understand where the greatest weaknesses are and direct resources to where the risk level is highest.

1.6. Data Collection

To assess the risks, information obtained from both official sources and public sources was relied upon. Key official sources included criminal statistics, court proceedings statistics, FIU reports and supervision statistics, Financial Supervision Authority supervision statistics, Internal Security Service information, Bank of Estonia internal and external payment statistics, and other state finance-related data, Tax and Customs Board control procedures and violations, as well as export and import data, and statistical data on legal entities from the Business register. All data used in the assessment were collected annually for the period 2020-2024.

Additionally, data from written surveys and focus group interviews with the private sector were used, including sector-specific data collected by professional organizations.

SUMMARY

The money laundering risk assessment is a study³ prepared in cooperation with state authorities and market participants, analyzing money laundering risks in Estonia. This is Estonia's third risk assessment, covering the years 2020-2024. The previous⁴, second national risk assessment report was prepared in 2021, based on data from 2017-2019. The very first national risk assessment was published in Estonia in 2015 and covered the three years preceding the second risk assessment period.

The risk level defined in the risk assessment depends on the interaction between threat and vulnerability. A threat is an event, activity, or pattern of activity that indicates the possibility that financial criminals will use the Estonian economic space and financial system to launder their proceeds. Vulnerability is a deficiency in the collection of various anti-money laundering measures, which constitutes the anti-money laundering system. The state participates in the anti-money laundering system through its legal framework and the tasks assigned to state authorities, and private sector companies also participate by complying with state laws and following the guidelines of state authorities, actively participating in the prevention process and cooperating with the state. The state's goal is to protect a fair competitive environment in the local economy, ensure the protection of the rights of all parties, and support the motivation of market participants to contribute to the fight against money laundering and maintain the country's good reputation.

The purpose of the risk assessment is to identify risks for which enhanced measures should be applied, as well as situations where simplified measures may be considered. In certain cases, it may be concluded that additional measures are no longer justified, and existing resources should be redirected to other areas. As a result of the risk assessment, a risk mitigation action plan is prepared, which is approved by the Anti-Money Laundering and Terrorist Financing Government Commission. The purpose of the action plan is to direct resources to mitigate and prevent priority risks, thereby limiting the opportunities to use the Estonian financial system and market participants for money laundering.

In the past five years, events have occurred worldwide that have impacted financial crime, including the COVID-19 pandemic and Russia's war of aggression against Ukraine. These events have significantly affected the Estonian economy, national and international cooperation, and the behavior of market participants. As a result, global risk trends have changed, necessitating updates to national anti-money laundering systems.

National Money Laundering Threats

The overall level of money laundering threat in Estonia has remained at a **medium** level over the past five years. The number of money laundering criminal cases in Estonia has remained stable, but the proceedings are complex and time-consuming. Most money laundering cases involved the layering stage, where criminal proceeds obtained abroad moved through the Estonian financial system. The main predicate offenses were fraud, especially BEC fraud, as well as tax and drug crimes. Companies registered in Estonia are often used to commit crimes abroad, particularly in the case of tax crimes.

³ See Chapter 1 for details.

⁴ The national risk assessments are published on the website of the Ministry of Finance:
<https://fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud>

In money laundering cases between 2020 and 2024, assets worth tens of millions of euros were seized and confiscated. Money laundering is often treated as a standalone crime, and proving it is complex, especially when predicate offenses are committed abroad. According to court practice, the criminal origin of the assets and the intent to conceal it are crucial in identifying money laundering. In Estonia, money laundering often involves the use of straw men, fictitious contracts, and cross-border bank transfers.

There is a growing trend of money laundering as a service, where criminal networks use intermediaries and service providers to conceal the origin of assets. Criminal networks in Estonia often operate on a project basis and are interconnected. In 2024, several groups involved in money laundering were identified, using cash and shell companies to conceal proceeds. High-risk sectors include cash-based sectors such as casinos, catering, and real estate. Criminal organizations use legal entities for both criminal and legitimate business activities, particularly in management and business consulting services. Money laundering mainly occurs through bank transfers, fictitious invoices, and loan agreements, but virtual currencies are increasingly being used. The risk level has also risen concerning companies registered in Estonia but with weak ties to Estonia, often managed by e-residents or foreign nationals.

Sectors with elevated money laundering threat levels include credit institutions, virtual currency service providers, corporate service providers, and, since 2023, gambling organizers. This means that money laundering cases have been observed in these sectors both nationally and internationally. If market participants have deficiencies in risk prevention and mitigation activities, the likelihood of such cases may increase. A higher-than-average threat assessment indicates that actors in these sectors need to pay more attention to anti-money laundering efforts and remain vigilant. It is also important for the state to direct appropriate supervisory resources to these areas and contribute to the prevention of money laundering cases.

The e-residency program itself does not create new money laundering risks but can make offenses easier and cheaper, especially in conjunction with the ease of establishing a company in Estonia, a tax-friendly environment, and a network of corporate service providers. Risks mainly manifest in foreign countries where companies created by e-residents may be abused. There have been few cases in criminal proceedings in Estonia, and there is no court practice. According to investigative authorities, 98.5% of e-residents and 94.2% of their companies are not involved in suspicious activities. However, individual e-residents may participate in extensive international schemes, causing reputational damage to Estonia. There are limited possibilities for background checks on third-country nationals. Several steps have been taken to mitigate risks between 2020 and 2024: stricter selection of target countries, enhanced pre- and post-controls, implementation of e-application environment and risk profile solutions, and more active deletion of companies that have not submitted annual reports.

Vulnerabilities of the National Anti-Money Laundering System

The vulnerability level of the national anti-money laundering system is **medium**.

Estonia's anti-money laundering framework has several strengths: regular national risk assessments, a clear focus on financial crime in the strategic documents of institutions, transparent and internationally compliant legislation. Operational-level cooperation is also effective, and public-private sector cooperation is strong.

Although the legal framework is robust and diverse, it is important to ensure uniform priorities, resources, and metrics for monitoring results within the system of institutions involved in anti-money laundering. The lack of a unified national strategy causes inconsistency between institutions and complicates resource planning.

Estonia's system for handling money laundering and financial crimes has developed on several levels in

recent years, but its capacity remains uneven and largely depends on human resources, the functioning of international cooperation, and technological support.

At the beginning of the period under review, in 2021, the Financial Intelligence Unit (hereinafter "FIU") was transformed into an independent government agency under the Ministry of Finance. The FIU's capacity for planning and conducting risk-based supervision has significantly increased. Both the FIU and the Financial Supervision Authority have substantially enhanced their capabilities in anti-money laundering supervision during the reporting period by increasing human resources and developing technical solutions. The FIU has strengthened its analytical and supervisory capabilities, and the Financial Supervision Authority has developed a risk dashboard system that enables targeted supervision.

During the period under review, the FIU has significantly improved the quality of reports received from market participants by focusing on targeted training and guidance in cooperation with other institutions. At the same time, risk awareness in many sectors has also increased. Improved information quality and the more extensive transmission of factual information by the FIU to investigative authorities have led to the initiation of several criminal proceedings.

Positive changes have also occurred in the work of the Prosecutor's Office and the Police and Border Guard Board. The Police and Border Guard Board and the Prosecutor's Office have increased their capacity by creating new positions and structural units, which has improved the ability to investigate and prosecute money laundering. The border and customs control system is generally strong, but bottlenecks in sanctions supervision and data processing capacity need attention.

The investigation and prosecution of financial crimes have been a priority for the Prosecutor's Office, as evidenced by structural changes in recent years. The complexity of identifying predicate offenses, as they are often committed outside Estonia, and the time-consuming nature of international cooperation, which is virtually non-existent with some countries, complicate the investigation of money laundering. The court system lacks specialization in handling money laundering cases, which prolongs the duration of complex proceedings. The effectiveness of conducting money laundering criminal proceedings is hampered by the high burden of proof, statute of limitations, and narrow interpretation of the concept of money laundering.

In several institutions, such as the Tax and Customs Board, the Security Police Board, and the Environmental Board, the capacity to handle money laundering is limited, and there are no units specialized in money laundering.

The legal framework for asset seizure and confiscation exists but needs updating and stronger implementation. Although the volume of seized and confiscated assets increased in 2023-2024, this was mainly due to a few large cases rather than systematic development. The Supreme Court has pointed out deficiencies in the law and emphasized the need for clearer regulation. Additionally, this area faces issues such as limited resources, uneven use of legal opportunities, and the costs of maintaining assets.

There is still room for improvement in the collection, processing, and analysis of national statistical data. The data are fragmented, inconsistent, and often not available in real-time, which complicates both operational and strategic decisions. This particularly concerns asset seizure and confiscation. There are shortcomings in data-based risk assessment and prevention, as well as in the ability to plan strategies based on data.

Sectoral Threats and Vulnerabilities

The risk level of sectors is determined by both threat and vulnerability. The threat level is influenced by the national money laundering threat, as well as typologies and sector-specific circumstances. The main components

of sectoral money laundering vulnerability include risk awareness, the quality of the implementation of due diligence measures, the presence of supervision, and the regulation of market access. At the sectoral level, factors such as the proportion of cash transactions, the presence of high-risk clients, and the anonymity associated with the service or product, as well as other technological aspects that limit transparency and complicate the proper implementation of due diligence measures, can increase the risk level.

In areas where the money laundering risk level is higher, both market participants and state authorities must apply a risk-based approach and pay greater attention to preventing criminals from using these sectors for money laundering.

Table 2. Results of the National ML Risk Assessment by Sector in 2025

Sector	Threat	Vulnerability	Residual Risk
credit institutions	above average	medium	medium
credit providers and intermediaries	medium	medium	medium
investment firms	medium	medium	medium
payment institutions and e-money institutions	above average	medium	medium
fund managers	medium	above average	above average
life insurance companies	low	low	low
savings and loan associations	medium	medium	medium
currency exchangers	medium	below average	medium
virtual asset service providers	above average	above average	medium
gambling organizers	above average	above average	high
lawyers	medium	medium	medium
notaries	medium	medium	medium
accounting and tax advisors	medium	medium	medium
other legal service providers	medium	medium	medium
traders	below average	high	medium
precious metal brokers	below average	medium	medium
real estate brokers	medium	above average	medium
audit firms	low	below average	low
company service providers	above average	above average	medium
bailiffs and bankruptcy trustees	low	below average	low
pawnshops	low	medium	low

The level of money laundering threat varies across sectors. Sectors with a higher-than-average threat level include credit institutions, payment and e-money institutions, virtual currency service providers, gambling organizers, and corporate service providers. Most other sectors fall into the medium-risk category. Sectors with a lower threat level include life insurance companies, auditors, and pawnshops. This distribution helps focus supervision and preventive activities on sectors where the threat level is higher and where the effectiveness of preventive measures is particularly important.

According to the risk assessment, the **higher threat and vulnerability levels are associated with gambling organizers** holding Estonian licenses, whose number has doubled in five years. The legal framework regulating companies in the remote gambling sector in Estonia has so far favored the acquisition of licenses even for companies with very little or no connection to Estonia. The use of virtual currencies in gambling for placing bets or withdrawing winnings also increases the risk level associated with the sector. The situation in the gambling organizers' sector is similar to the risk picture identified in the 2021 risk assessment for virtual currency service providers. After the previous risk assessment, mitigating the risks associated with virtual currency service providers was prioritized, and the risk mitigation measures effectively regulated the market, significantly reducing the sector's vulnerability level.

The level of money laundering vulnerability in sectors is generally **medium**, but some areas have higher or lower vulnerability levels. According to the assessment, fund managers, gambling organizers, real estate brokers, and corporate service providers are more vulnerable, as the complexity and international scope of their services or client anonymity can complicate the effective implementation of due diligence measures.

The vulnerability level of traders to money laundering is assessed as high, indicating that despite the higher money laundering risk, there may be significant deficiencies in risk prevention or control mechanisms in this sector. The new EU anti-money laundering regulation⁵ will bring significant changes to the definitions of cash payments and obliged entities. As a result, traders will no longer be considered obliged entities in the future, except when dealing with high-value goods or the sale of precious metals and stones. Therefore, only higher-risk activities will remain within the scope of obliged entities, creating conditions for more targeted and effective supervision and reducing the sector's vulnerability level.

Most sectors have a medium level of money laundering vulnerability, including credit institutions, investment firms, lawyers, notaries, accountants, legal service providers, and other professional and financial sector sub-sectors. In these sectors, the level of vulnerability largely depends on how consistently and effectively risk-based control measures are implemented.

Sectors with a lower level of money laundering vulnerability include life insurance companies, audit firms, bailiffs and bankruptcy trustees, and pawnshops, where the money laundering risks associated with products and services are less likely.

Representatives of non-financial sectors, i.e., freelancers and professionals, play a gatekeeper role in preventing money laundering: corporate service providers, lawyers, accountants, real estate agencies, notaries, etc. The **gatekeeper role in non-financial sectors** is that they are often the first to encounter client activities that may be related to money laundering. Due to their position, they can identify suspicious transactions or schemes early on. Therefore, their role in preventing money laundering is critical – they act as a filter that helps prevent the movement of illegal money into the financial system.

It is also important to consider that companies registered in Estonia may be used for money laundering purposes, including internationally. Although the **risk of companies being used for money laundering is assessed as medium**, it still has a significant impact on the reliability of Estonia's financial system and the country's reputation. Therefore, the role of professionals and freelancers is extremely important – their conscious and responsible actions help ensure that no company maliciously created for money laundering and its predicate offenses reaches the Estonian financial system and damages the country's international reputation. It is crucial that the reporting activity and the quality of due diligence measures in higher-risk areas increase in the near future.

⁵ AMLR 2024/1624 article 80 and article 3, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401624

Residual money laundering risk is the risk that remains after all relevant preventive and deterrent measures have been implemented. It reflects the assessment of how likely money laundering is to occur despite existing controls, supervision, and due diligence measures. The level of residual risk is influenced not only by the effectiveness of preventive measures but also by the materiality of the sectors – for example, the number of obliged entities, the total turnover of the sector, or its share in the financial system. In larger sectors, the residual risk may be more significant because the potential impact in the event of a money laundering case is greater. Although the money laundering threat and vulnerability of the gambling organizers and corporate service providers sectors are assessed at the same level, their residual risk levels are different. This is due to the size of the sector – in the larger, more impactful gambling sector, the residual risk level is higher, while in the smaller company service providers (hereinafter “CSP”) sector, it remains medium. This approach helps direct supervision and resources to where the impact of risk realization would be the most extensive.

Recent global trends highlight the need to consider the rapid development of technology. The use of artificial intelligence has increased, bringing risks such as deepfake technology, which facilitates identity fraud and threatens know-your-customer⁶ processes. All market participants must contribute more to mitigating fraud-related risks, especially when using automated KYC solutions and when employing separate service providers to determine whether they have sufficient capability to handle deepfake technology.

This risk assessment provides a detailed description of money laundering threats and vulnerabilities. The assessment highlights new issues and tasks that require a risk-based approach and additional measures to strengthen the ability to prevent money laundering and direct resources to areas with higher risk levels.

The risk assessment report presents several risk typologies and describes cases from which both market participants and state authorities can learn. Specific recommendations are given to obliged entities on how to enhance the fight against money laundering.

The study results provide a strong foundation for developing a further national action plan and strategy. The post-risk assessment action plan sets priorities and focuses on areas with higher-than-average risk levels.

⁶ KYC or Know-Your-Client.

Abbreviations

BEC fraud	– a scam where the perpetrator poses as an employee of a trusted company (e.g., a manager or partner) to extract money or sensitive information from the victim via email
EB	– Environmental Board
FIU	– Financial Intelligence Unit
ISA	– International Sanction Act
ISS	– Internal Security Service
JDM	– Ministry of Justice and Digital Affairs
KYC	– Know Your Customer principle
MAA	– Annual Report of Economic Activity
ML	– Money Laundering
MLTFPA	– Money Laundering and Terrorist Financing Prevention Act
MoF	– Ministry of Finance
MoI	– Ministry of Interior
NRA	– National Risk Assessment
PenC	– Penal Code
PF	– Financing of the Proliferation of Weapons of Mass Destruction
TCB	– Tax and Customs Board
TF	– Terrorist Financing
VASP	– Virtual Currency Service Provider

The types of reports to the FIU are as follows:

CTR	– cash transaction report
ISR	– international sanction report
STR	– suspicious transaction report
TR_UAR	– unusual activity report (TF)
TFR	– terrorist financing report
UAR	– unusual activity report
UTR	– unusual transaction report (ML)

2. National ML Threats

2.1. Description of the Methodology

To assess money laundering threats, three sub-modules of the World Bank methodology were used, which together form a comprehensive threat analysis framework.

Table 3. Modules used in the assessment of national money laundering threats

National Level	Module used in the assessment
Money Laundering Threats	Module 1.A ML Threat Assessment, Module 1.B ML Case Based Assessment, Module 1.C Crossborder ML Threat

1.A – General Assessment of Money Laundering Threat

This module focused on assessing the sources and extent of criminal proceeds domestically. It evaluated which types of crime generate the most revenue and their impact on money laundering threat. The results provided an overview of the likelihood of money laundering occurring within the country.

1.B – Case-Based Assessment

In this module, actual money laundering cases were analyzed to understand how money laundering occurs in practice. The methods used, the sectors involved, and international connections were evaluated based on the cases. This provided a substantive dimension to the risk assessment, relying on real experience and data.

1.C – Cross-Border Money Laundering Threat

This module focused on money laundering risks associated with international transactions and cross-border criminal networks. It assessed the likelihood of criminal proceeds moving in or out of the country and the channels and mechanisms that facilitate this.

In addition to the assessment modules included in the World Bank methodology, additional working tables were prepared and used by the working group in their assessments. These supplementary documents helped the working group structure discussions, support the evaluation of criteria, and ensure the accuracy and transparency of the results.

Both qualitative and quantitative data were used in the assessments: the experience and opinions of the working group experts, criminal statistics on predicate offenses for money laundering, court decisions on money laundering cases, statistics on the proceedings and information exchange of supervisory and law enforcement agencies, statistics on incoming and outgoing international inquiries, statistics on asset freezing and confiscation, and statistics from the Bank of Estonia on incoming and outgoing financial flows by country.

2.2. National Threats

2.2.1. The state of ML threats from 2020 to 2024

The threats of money laundering have remained at a **medium level** from 2020 to 2024. In cases of money laundering occurring in Estonia, it **mainly** involves the **layering stage**, where criminal proceeds from crimes committed abroad are layered within the Estonian financial system. Assets of unknown origin are moved into or through the Estonian financial system to another country's financial system, including **cash transactions**⁷.

Based on inquiries received by the FIU and the Police and Border Guard Board, as well as criminal cases initiated by investigative authorities in Estonia concerning money laundering (Penal Code § 394), the main predicate offense for money laundering is **fraud**. In addition to fraud, predicate offenses for money laundering also include **drug, tax, and professional**⁸ crimes.

Due to the Russian Federation's aggression against Ukraine, which began on February 24, 2022, and the subsequent imposition of European Union sanctions, there may be an increase in cases where sanctions violations are treated as predicate offenses for money laundering in the future. This particularly concerns cases where financial resources are made available to persons or entities subject to sanctions. Although the flow of funds from eastern countries decreased in 2023, resulting in a reduction in the **movement of criminal money into the Estonian real estate sector**, an increase in real estate investments, including the use of cash, was observed again in 2024. This means that the threat of money laundering in the real estate sector still exists and is rather increasing.

From 2020 to 2024, the sectors with a higher than average threat level were **credit institutions and agents and service intermediaries of foreign payment institutions and e-money institutions** operating in Estonia (primarily in the provision of cross-border payment services) and **virtual asset service providers**. Since 2022, the threat of money laundering has been higher than average in the **company service provider** sector, and since 2023, in the **gambling sector**.

⁷ Commentary on the Penal Code 2021, p. 1119, section 12: Cashing is a transaction or activity that results in the conversion of non-cash value or payment instrument into a bearer payment instrument. Bearer payment instruments include financial instruments such as traveler's checks, freely tradable payment instruments (including checks, bonds, and money orders) that are either unrestrictedly endorsed and made out to the bearer or in some other form that ensures the transfer of ownership upon delivery, and incomplete payment instruments (including checks, bonds, and money orders) that are signed but the payee's name is not specified, as well as banknotes and coins that are in circulation as a means of payment.

⁸ Professional crimes, i.e., bribery (giving, mediating, taking).

Table 4. Sectors involved in ML cases and ML risks over the years

Year	ML risk level	ML stage	Predicate Offences	Sectors
2021	Medium	Layering stage	Fraud and tax crimes, drug	Sectors with a higher-than-average threat level: credit institutions, virtual asset service providers
2022	Medium	Layering stage	Fraud and tax crimes, as well as cyber, drug, corruption crimes, and embezzlement	Sectors vulnerable in the layering phase: virtual asset service providers and company service providers; vulnerable sector in the integration phase: real estate agents
2023	Medium	Layering stage	Fraud, sanctions evasion, tax crimes	Sectors with a higher-than-average threat level: credit institutions, virtual asset service providers, and company service providers
2024	Medium	Layering stage	Fraud, tax crimes, sanctions evasion	Sectors with a higher-than-average money laundering threat level: credit institutions, cross-border payment services, virtual asset service providers, company service providers, and gambling operators

Source: PBGB

Some corporate service providers have created services that make it easier to conceal the true beneficiaries and related persons of companies. These services are also used by e-residents or foreign nationals. Based on information received by the FIU and investigative authorities from competent authorities in foreign countries, submitted international legal assistance requests, and information exchanges, it can be concluded that some companies registered in Estonia have been involved in crimes, including tax offenses, committed outside of Estonia. It is important to emphasize that this **does not apply to all companies** registered in Estonia, but mainly to those legal entities with weak ties to Estonia – they lack a permanent place of business in Estonia and are often managed by e-residents or foreign nationals who do not live in Estonia and have no (permanent) connection to Estonia. Most of these companies have been established by corporate service providers. It should be noted that the situation picture obtained from foreign inquiries reaches Estonia with a delay, so by the time the inquiry is made, the company’s activity license may already be invalid or in the process of being revoked. It can be expected that this trend will continue in the future.

Underground Banking

Ongoing criminal proceedings and information gathered by investigative authorities reveal that **underground banking** (IVTS)⁹ operating parallel to the conventional financial sector continues to cause problems and poses a **high threat** of money laundering. The mentioned proceedings are still ongoing, and no final court decisions have been made yet. Estonian companies and individuals wishing to conceal their criminal activities are increasingly using the opportunities offered **by cross-border payment or e-money service providers** to conduct cash transactions.

⁹ Informal value transfer system. Known by various names, such as Hawala, Hundi, etc.

Cash

The use of cash among the Estonian population is generally decreasing, with a preference for electronic payments¹⁰. However, the number of reports sent to the FIU indicating cash-related transactions sharply increased in 2024, doubling compared to previous years. This suggests that the level of money laundering risk associated with cash remains high and requires continued attention. Cash remains significant, as criminals increasingly direct it into virtual currencies. For example, money laundering service providers are used to convert criminally obtained funds into crypto assets.

Money laundering as a service

According to a Europol study, the role of **financial and legal advisors** in companies associated with criminal networks is significant due to their international activities¹¹. These networks' activities include laundering proceeds from crime, making service providers key players in committing money laundering offenses. In 2024, investigative authorities focused increased attention on the activities of service providers, registering five cases of money laundering offenses related to money laundering services and/or aiding money laundering.

Companies with a higher money laundering risk

Individuals associated with companies with a money laundering risk are predominantly foreign nationals, among whom a significant proportion are e-residents and persons with unknown or undefined citizenship. Most frequently, companies with a money laundering risk were associated with individuals from Ukraine and Russia.

The majority (76.2%) of individuals associated with companies that failed to submit their annual reports are **foreigners**. Among them, the largest share consists of **persons with unknown or undefined citizenship** (41.6%), followed by citizens of Russia (2.7%), India (2.5%), and Ukraine (2.3%); the proportion of e-residents is 30%.

In summary, several money laundering-related threats persist in Estonia, including cross-border money laundering schemes, money laundering as a service, cash transactions, threats arising from corporate service providers, gambling operators, and virtual currency service providers, among many other risk factors. The FIU and investigative authorities are addressing these risks through supervision, cooperation, raising awareness, and criminal proceedings.

2.2.2. Sectors with a threat level above average

All sectors considered as obligated entities¹² were examined. The following sections will review sectors with a higher-than-average threat level and explain the factors causing this threat. Other sectors exhibit either an average or low level of money laundering threat¹³.

¹⁰ <https://www.eestipank.ee/press/uuring-eestis-kasutatakse-maksmisel-enim-digitaalseid-maksevahendeid-14012025>

¹¹ Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures, 18. detsember 2024, p 10.

¹² MLTFPA § 2. <https://www.riigiteataja.ee/akt/113032019126?leiaKehtiv>

¹³ The money laundering threat levels for all sectors are presented in the Summary, Table 1.

Credit Institutions

Payment services offered by credit institutions, especially correspondent services to foreign FinTech¹⁴ companies, remain the most vulnerable to cross-border criminal proceeds layering.

Since 2020, the movement of funds obtained through fraud via virtual bank accounts (**VIBANs**¹⁵) has increased, becoming a noticeable trend. Cases of sanctions evasion are predominantly associated with credit institutions.

In 2021, cases related to correspondent accounts opened in Estonian credit institutions accounted for 32% of the FIU's incoming foreign communications. Although the number of reports decreased in absolute terms by the end of 2024, this was influenced by the decision of certain correspondent institutions to terminate business relationships with specific respondent institutions, indicating a reassessment of risks in the sector.

VASPs

In general, the number of market participants among virtual currency service providers (VASPs) licensed in Estonia has decreased (as of 31.12.2024, there are only 42 service providers), and the reduction in information and foreign inquiries about them indicates a lower risk level. However, the risk has concentrated among a few market participants, especially those serving crypto casinos.

Virtual currencies continue to be used to conceal criminal proceeds – in 2024, \$24.2 billion¹⁶ related to illegal activities moved to associated accounts. The overall risk level of service providers licensed in Estonia has decreased compared to the years 2017–2019, but the risk has concentrated among service providers serving online casinos. Previously, VASPs had deficiencies in risk assessment, but by 2024, their overall understanding of risks has improved. This is evidenced by the reduced amount of information received about them (by the FIU and law enforcement agencies) and the number of foreign inquiries. Problems persist with identifying clients and fulfilling the obligation to determine the origin of clients' funds.

Gambling Sector

In the gambling sector, remote gambling operators and companies associated with foreign nationals or foreign entities dominate in terms of both volume and money laundering risks. Since 2020, the number of market participants, the volume of services, and the associated risks in the gambling sector have grown significantly¹⁷. There has been a notable increase in remote gambling operators with an international clientele. The growth in service volume is driven by non-resident clients. In 2024, the FIU emphasized the risk associated with gambling operators, particularly remote gambling operators or online casinos. According to published international studies and typologies, gambling operators are increasingly involved in laundering proceeds from crime.

¹⁴ Fintech, or **financial technology**, is a field that combines financial services and new technology with the aim of improving, automating, and making financial activities more efficient and user-friendly. This includes, for example, digital payment systems, mobile banking, investment platforms, lending services, cryptocurrencies, blockchain technology, and much more, which help make money management easier and faster.

¹⁵ FIU Yearbook 2023.

¹⁶ Chainalysis Crypto Crime Report 2025.

¹⁷ FIU Yearbook 2024.

Company Service Providers

The risk level of company service providers remains higher than average, and the sector is characterized by low risk awareness. Companies created through Estonian company service providers continue to be used for criminal purposes, including international organized crime. The risk of misuse of these companies increases with the scope and availability of the services offered, especially those aimed at non-residents. Service providers often participate in the creation and management of shell companies that are abused internationally.

Many of them offer services to non-residents whose companies fall into the medium or high-risk category. Most of these companies do not actively operate in Estonia, which is an additional red flag. Based on studies and foreign inquiries received by the FIU, it has been found that most companies associated with non-residents, which lack both a bank account and business activities in Estonia, were created through company service providers. It has also been identified that these companies are used in money laundering schemes and other international crimes.

In 2024, the threat of misuse of legal entities decreased thanks to the business register's ability to delete companies that show no signs of activity. Common typologies indicating layering stage activities include transit transactions between legal entities with accounts opened in different jurisdictions that have the characteristics of shell companies, and fictitious loan transactions.

Violations have emerged in the sector, including the deliberate disregard of due diligence obligations, which creates opportunities for the movement of funds of dubious origin into the financial system of Estonia and the European Union. According to information received from foreign countries, companies registered in Estonia are often used to commit crimes outside of Estonia, including tax offenses. These companies often have no connection to Estonia – they are associated with e-residents or foreign nationals who do not live or operate in Estonia. Assessing the situation is complicated by the fact that information obtained through foreign inquiries often arrives with a delay, and the company's status may have already changed by the time the inquiry is made. Given the current trends, it can be expected that this phenomenon will continue in the future.

2.2.3. Provision of the ML services in organized crime

Cash plays a significant role in the context of money laundering, which is why the risk level is higher in business sectors where cash is extensively used – for example, in casinos, catering businesses, and the real estate sector. Shell companies are also often used for laundering cash.

It is increasingly common for criminal groups to intertwine their activities with legal entities, which are used for both criminal activities, including money laundering, and legitimate business operations. Notable areas include **business and management consulting**.

Expert knowledge has identified that some criminal groups collaborate in the field of money laundering – for instance, one group may provide **money laundering services** to another when needed. Therefore, it is important to consider money laundering in the context of organized crime as a separate service. Criminal organizations primarily use traditional money laundering methods, such as bank transfers based on fictitious invoices¹⁸ or loan agreements. **Cash** still plays an important role, but it is increasingly being directed into **virtual currencies**. For example, money laundering service providers are used to convert criminally obtained funds into virtual currencies. Conversely, the opposite process has also been observed, where virtual currencies are converted into cash, known as **“cash-out” transactions**.

¹⁸ A fictitious invoice is an invoice that does not reflect an actual economic transaction.

2.2.4. ML cases processed in 2020–2024

The number of criminal cases related to money laundering under investigation by law enforcement agencies has remained generally stable. Year-to-year fluctuations are primarily due to the availability of investigative resources and the complexity and time-consuming nature of money laundering cases. Since money laundering is a difficult-to-detect hidden crime, the number of registered cases is relatively small. The number of investigations is positively influenced by the fact that money laundering prevention has been prioritized in several Estonian investigative and supervisory authorities, as well as the prosecutor's office. The importance of the issue is also emphasized in strategic documents, such as the Ministry of the Interior's Internal Security Development Plan for 2020–2023, the Prosecutor's Office's 2024 Annual Report, and the Financial Supervision Authority's Money Laundering Prevention Supervision Strategy for 2022–2025.

In 2020–2021, 16 money laundering criminal cases were initiated, involving a total of 17 registered crimes. Approximately 29.6 million euros were under investigation. One case involved a corporate service provider who provided services to non-resident virtual currency companies. These services included company formation, provision of a contact person and address, and applying for Estonian licenses. Such companies may be used for computer crimes and investment fraud. 27.8 million euros were related to a criminal case that originated from a crime report received from the FIU concerning the embezzlement of state budget funds in Ukraine. From 2015 to 2018, funds suspected of money laundering moved from foreign companies' bank accounts to the accounts of an Estonian company. The case involves a money laundering service provider residing in Estonia, who has also received a foreign inquiry from Sweden, where a 10 million euro money laundering suspicion is under investigation. The individual has established companies both in Estonia and abroad and held bank accounts in several countries through which suspicious funds moved. Extensive criminal information has been received regarding money laundering services offered through **Estonian company service providers**, and several foreign inquiries have identified cases where companies associated with these service providers were used. The remaining 1.8 million euros mainly concern eight criminal cases where the predicate offenses were computer fraud amounting to 1.4 million euros. In these cases, the parties were involved in the **use of virtual currencies**¹⁹.

In 2022, 16 criminal proceedings related to money laundering were initiated in Estonia, seven of which were initiated in cooperation with the FIU. This number is higher than in previous years. Most of the proceedings address money laundering as the main offense, but money laundering has also occurred in conjunction with fraud, drug crimes, causing insolvency, document forgery, and unlicensed economic activities. The FIU forwarded five crime reports to the Police and Border Guard Board (PBGB): in two cases, proceedings were initiated for unlicensed and prohibited economic activities, in one case for providing false information, in one case for money laundering, and in one case no proceedings were initiated. **Seven criminal cases were forwarded to the prosecutor's office for further proceedings, and by the end of the year, a total of 28 money laundering criminal cases were under investigation.** In 2022, assets worth over 29 million euros were seized in criminal cases forwarded to the prosecutor's office, of which approximately 4% was cash. In the same year, assets worth 2.6 million euros were seized, of which 21.5% was cash. In total, approximately 7.3 million euros were seized in criminal cases under investigation in 2022, of which 7 million euros were seized in 2022 alone – the share of cash was 0.03%. These are record amounts compared to previous years. In cases forwarded by the FIU to the PBGB, financial assets totaling over 11 million euros were restricted. In four cases, criminal proceedings were initiated, where the FIU restricted assets worth over 7 million euros²⁰.

¹⁹ PBGB, Money Laundering Crime Situation Report 2021, 15.12.2021.

²⁰ PBGB, Money Laundering Crime Situation Report 2022, 18.04.2023.

According to the PBGB's 2023 serious hidden crime threat assessment, the **money laundering threat in Estonia is medium**. As of 31.01.2024, the PBGB is investigating 22 money laundering criminal cases, most of which (14) are solely related to money laundering, but the adjacent offenses include causing insolvency, fraud, embezzlement, and computer fraud in at least two cases (PRIS data).

In 2023, **fewer money laundering criminal proceedings and cases were registered** compared to previous years. According to ALIS data, only 5% of serious hidden crimes registered in 2023 were economic crimes, of which money laundering crimes accounted for 7.5% (11 crimes). Of the 11 cases, money laundering criminal proceedings were initiated in nine, spanning seven criminal cases. Six money laundering criminal cases were initiated in 2023. It is known that at least one criminal case did not initiate money laundering and money laundering agreement cases. The North Prefecture Criminal Bureau KMT handles most money laundering criminal cases, primarily **in cooperation with the FIU**. Economic crimes accounted for about 5.5% of serious hidden crimes sent to the prosecutor's office in 2023, of which money laundering cases made up about 16% (7).

Court practice in money laundering criminal cases is limited. In 2023, four County Court decisions on money laundering became final, all of which involved BEC fraud as predicate offenses. The predicate offenses in ongoing money laundering criminal cases are also predominantly fraud (investment fraud, phone fraud), but the concept has become more complex. There are still difficulties in **identifying and proving the predicate offense** in money laundering criminal cases. The predicate offenses are mostly committed abroad, but collecting evidence from foreign countries is time-consuming, and cooperation varies by country²¹.

In 2024, the PBGB had a total of 22 criminal cases with money laundering qualifications under investigation. During the year, 11 new money laundering criminal cases were initiated, and 18 money laundering crimes were registered, divided among 15 different criminal cases. These registered crimes accounted for approximately 20% of all serious corruption and economic crimes.

Five registered cases were related to providing money laundering services or aiding money laundering. A total of five money laundering crimes were forwarded to the prosecutor's office, three of which were registered in 2024. Seven individuals and two legal entities were sent to the prosecutor's office as suspects in three different criminal cases. The legal entities were involved in wholesale trade and the provision of corporate services.

Four criminal cases reached the court, involving a total of six defendants. The predicate offenses for money laundering crimes in 2024 were mainly fraud, including investment fraud. Additionally, there were cases related to causing insolvency, cybercrime, and smuggling.

The predicate offenses were often committed abroad, particularly in Finland, Lithuania, and Ukraine. Notably, fraud schemes have become more complex over the years, and alternative financial channels, such as underground banking, payment intermediaries, and virtual currencies, are increasingly used to move criminal proceeds.

One of the biggest challenges in handling money laundering crimes remains proving the predicate offenses, especially in cases where they are committed in jurisdictions that do not cooperate with Estonia, such as Russia. The concept of fraud as a predicate offense has become more complex over the years. Instead of banks, alternative channels like underground banking, payment intermediaries, and virtual currencies are increasingly used to move criminal proceeds.

²¹ PBGB, Money Laundering Crime Situation Report 2023, 09.02.2024.

Money laundering can be classified into three types. **Stand-alone or autonomous money laundering** occurs when charges are brought solely for the money laundering offense, without simultaneously charging for the predicate offense.²² **Third-party money laundering** involves situations where the person who engages in concealment activities with the proceeds of the predicate offense did not participate in the commission of the predicate offense. **Self-laundering** occurs in cases where the person involved in the commission of the predicate offense begins to carry out concealment activities with the proceeds of the predicate offense themselves.²³

According to Estonian law, the object of money laundering can originate from any crime, but it is required that the crime resulted in the acquisition of assets. The Supreme Court has clarified that for the purposes of the composition of § 385 of the Penal Code, it is not important whether the debtor acquired the assets legally or illegally.²⁴ However, the origin of the assets is crucial in assessing the fulfillment of the composition of § 394 of the Penal Code. This composition is fulfilled only by laundering assets obtained as a result of criminal activity. For example, if person A legally acquires a car but forges documents related to the car, the car does not become criminal property, even though it is seemingly connected to a crime through forgery. Similarly, it is not sufficient to charge someone with money laundering if the origin of the car is unknown; it must be proven that the assets are derived from a crime. The question remains as to how the criminal pre-activity must be proven. The Penal Code lists 62 criminal compositions that allow for extended confiscation (§ 83² of the Penal Code).²⁵

The Penal Code lists a total of 62 criminal compositions for which extended confiscation can be applied (§ 83² of the Penal Code). This list encompasses the entire relevant legal framework. The working group experts selected **47** of these compositions based on substantive risk assessment and practical significance, not just the possibility of confiscation. The selection did not focus solely on high-risk provisions, as the possibility of extended confiscation does not automatically mean that the crime is high-risk or that criminal proceeds are always present. The working group based their selection on the characteristics of the composition set out in § 394 of the Penal Code and the practice of the Supreme Court, identifying **those compositions where perpetrators are likely to earn significant criminal proceeds**. Such proceeds are not immediately directed to final consumption; instead, criminals have the need and intention to conceal their illegal origin using the financial system – this is the essence of money laundering.

In cases with the qualification of the 47 criminal compositions selected by the working group, a total of **47,160 criminal cases** were initiated between 2020 and 2024, of which 9,780 were sent to the prosecutor's office, and assets worth **€61,251,824.19 were seized**. **6,460 criminal cases** ended with a conviction, with 9,754 individuals convicted, and assets worth **€12,132,096.04 were confiscated**.

As a side note, the amounts reflected in reports sent to the FIU related to suspected money laundering are increasing. In 2024, the FIU's money laundering-related information transmissions to investigative authorities included suspicious transactions worth a total of €222 million (a decrease of 19% compared to €314 million in 2023; the number of information transmissions decreased from 116 to 94, a 29% decrease²⁶)²⁷. In cases forwarded by the FIU to investigative authorities, the most significant predicate offenses were sanctions

²² Council of Europe. Typologies Report on Laundering the Proceeds of Organised Crime, p 117. <https://rm.coe.int/typologies-report-on-laundering-the-proceeds-of-organised-crime/168071509d>

²³ *Ibid.*, p 116.

²⁴ RKKKm 3-1-1-24-17, p 11.

²⁵ According to § 83² of the Estonian Penal Code, extended confiscation can be applied, meaning that the court may confiscate assets obtained through criminal activity even if the connection of the assets to a specific crime is not established, but there is reason to believe that the assets were acquired through criminal means. Extended confiscation can only be applied if the person is convicted of a crime for which the law allows such confiscation (e.g., money laundering, fraud, human trafficking, etc.).

²⁶ The processing of information received by the FIU for information transmission has a certain delay.

²⁷ FIU Yearbook 2024, p 22.

evasion, tax crimes, and fraud. The FIU still sent the most reports on so-called autonomous money laundering cases, where there were no direct references to predicate offenses, but the activity pattern suggested that it could be money laundering. However, the proportion of such cases has significantly decreased over the years.

During the same period, **27 criminal cases**²⁸ with money laundering qualifications were sent to the prosecutor's office, in which assets worth a total of **€8,791,497 were seized**, and assets worth a total of **€2,627,561 were confiscated**. In total, 808 criminal cases were sent to the prosecutor's office, in which assets worth a total of **€128,858,173 were seized**.

Although the definition of the object of money laundering has changed somewhat, the court practice regarding the requirements has been fairly consistent. The Tartu Court of Appeal noted in decision No. 1-18-8474, point 358, that until November 26, 2017, the object of the crime was "property obtained as a result of criminal activity or property obtained in place of it." From November 27, 2017, the object of the crime is "property obtained from criminal activity or property obtained in place of it." The Court of Appeal notes that nothing was said about such a change in the explanatory memorandum of the law, and the court is convinced that replacing the wording "as a result of criminal activity" with the phrase "from criminal activity" has no substantive meaning and the new law did not bring any changes regarding the object of money laundering.

Identifying, seizing, and confiscating criminal proceeds is an essential part of criminal proceedings, aimed at limiting the use of criminal proceeds for committing new crimes and ensuring a preventive effect. These measures are particularly important for hidden crimes (such as money laundering), where criminal assets are often deliberately concealed or converted. During such proceedings, parallel financial investigations are conducted to assess the volume and origin of assets controlled by individuals and legal entities and to carry out seizures to ensure the confiscation of assets.

As of December 31, 2024, there were a total of **58 criminal cases** with money laundering qualifications in pre-trial proceedings, of which 48 criminal cases involved one predicate offense of **fraud**²⁹. There have been no significant changes in the predicate offenses compared to the previous national risk assessment period. The predicate offenses of registered money laundering crimes were **mainly frauds committed abroad** (predominantly in Finland, Lithuania, and Ukraine). Additionally, predicate offenses include causing insolvency, cybercrimes, and smuggling.

The modus operandi and proof of fraud as a predicate offense have become more complex over the years, as alternative channels are increasingly used to move criminal proceeds instead of banks, making it difficult to identify the origin, owner, and actual beneficiary of the assets (underground banking, payment intermediaries, virtual currencies, etc.). Similarly, there are problems in Estonia with proving predicate offenses in money laundering cases, which is particularly challenging in cases where the predicate offense was committed in a jurisdiction that does not cooperate with Estonia (e.g., Russia)³⁰.

Between 2020 and 2024, **32 court decisions** were made in criminal proceedings with money laundering qualifications, of which **20 were convictions**. The activities of the legal entities involved in the proceedings were mainly wholesale trade and the provision of corporate services. A total of **51 individuals were convicted of money laundering**. **No legal entities were convicted**, as they were treated as instruments for committing the crime in these proceedings. The predicate offenses for money laundering included various frauds, including computer fraud and **business email compromise (BEC) fraud**.

²⁸ As of February 17, 2025, based on the data from investigative authorities and the prosecutor's office (summarized number, row 57).

²⁹ As of February 17, 2025, based on the data from investigative authorities and the prosecutor's office.

³⁰ For example, the termination of the Swedbank criminal proceedings. <https://www.err.ee/1609267686/prokuratuur-lopetas-swedbanki-rahapesukahtluse-kriminaalasja>.

CASES³¹:

- An individual was convicted in a plea agreement for using a forged important identity document and money laundering, which they committed repeatedly and on a large scale as part of a group. Acting with unidentified individuals during the pre-trial investigation, they concealed the criminal origin of the money and its connections to the perpetrators of the crimes through various activities (e.g., converting and transferring money) with the aim of directing the obtained money into the legal economy. The defendant allowed the use of companies they managed (D OÜ, V OÜ, X OÜ) and personal bank accounts, where criminally obtained funds were deposited. They then conducted transactions through these accounts to conceal the origin of the money. The criminal proceeds mainly originated from BEC frauds committed abroad. The money moved through Estonian companies and personal accounts to the accounts of straw persons or was withdrawn in cash to conceal its illegal origin.
- An individual was convicted in a plea agreement for money laundering, which they committed repeatedly and on a large scale as part of a group. They acted in cooperation with a Nigerian citizen living in Slovakia, under whose instructions the criminal origin of the money obtained through BEC frauds (business email compromise frauds) committed abroad was concealed through various transactions. To implement the criminal plan, the defendant sought legal and natural persons (straw persons) in Estonia, in whose names and through whose accounts the criminal money was moved. The money was transferred to the accounts of Estonian companies and then to other accounts or withdrawn in cash using fictitious contracts. The aim was to conceal the illegal origin of the assets and their connection to the predicate offenses.
- Three individuals were convicted in a plea agreement for aiding and abetting money laundering, which was committed repeatedly and on a large scale as part of a group. Within the criminal scheme, the origin of the money previously obtained through fraud and the connections of the criminals were concealed with the aim of directing these funds into the legal economy. The individuals involved in the scheme registered companies in their names and opened bank accounts for them, the details of which (including ID cards, passwords, and bank documents) were passed on to third parties. This allowed them to conduct transactions with criminally obtained money. They also sought individuals willing to register companies and open accounts in their names to conceal the illegal origin of the funds and facilitate their movement between the accounts of companies and individuals in Estonia, the United Kingdom, and the United States.

Considering the above Estonian statistical data, it should be emphasized that the small number of money laundering criminal cases compared to the total number of possible predicate offenses and the volume of seized assets is partly due to the legal interpretation of the composition of money laundering. According to criminal law and the practice of the Supreme Court, money laundering under § 394 of the Penal Code should be considered a harm offense, **aimed at protecting the state's financial and economic system from the integration of criminally obtained assets into the legal economy**. The legislator has not set the criminal law objective of criminalizing any use of criminally obtained assets as money laundering, but only such behavior that is aimed at concealing the origin and true owner of the assets in a way that endangers the integrity of the financial or economic system. Consequently, actions that involve the use of assets for immediate personal consumption, such as directing criminally obtained assets into direct final consumption, and that have no connection to the exploitation of the financial system, are not considered money laundering. Similarly, small-scale transactions that formally may meet the criteria of money laundering but do not have an actual

³¹ Harju County Court's decision of February 1, 2023, No. 1-23-250, decision of March 2, 2023, No. 1-23-654, and decision of March 9, 2023, No. 1-22-7110.

impact on the financial system are not considered money laundering. The Supreme Court has emphasized that the concealment of the origin and true owner of the assets, characteristic of money laundering, must be the central or primary objective of the actions taken with the assets. If this aspect is present only as a secondary objective or consequence, it is not considered money laundering under § 394 of the Penal Code (see RKKKo 3-1-1-85-11, 3-1-1-68-10, p 13; 3-1-1-34-05, p 25).

Table 5. Threshold values for due diligence measures according to § 19 of the MLTFPA

Application Situation	Threshold	Notes
Occasional transaction outside a business relationship	€15,000	Applies to both a single payment and multiple related payments within 1 year
Trader cash transaction	€10,000	Applies to receiving or paying cash in one or multiple related payments per year
NPO, foundation, or other non-profit entity cash transaction	€5,000	Applies to paying or receiving cash in one or multiple related payments within one year
Mediation of real estate use transaction	€10,000 per month	If the value of the usage fee is at least €10,000 per month
Transaction or storage of artwork in a customs free zone	€10,000	Applies to one or multiple related payments within one year
Gambling organizer's bet or payout	€2,000	Applies to both placing a bet and paying out winnings within one month

Additionally, it is important to note that according to the practice of the Supreme Court, the court relies on the threshold values for due diligence measures set out in § 19 of the MLTFPA when determining the threat to the financial and economic system in money laundering cases (see Table 5). The court practice holds that the legislator has considered transactions exceeding the defined amounts to be potentially dangerous for the financial and economic system. Consequently, the court practice has developed in such a way that, generally, it is not justified to treat the handling of criminal proceeds below the specified value as money laundering, except in cases where other significant risk factors are present.

2.2.5. Trends in ML threats identified in international cooperation

During the observed period, Estonia participated in a total of **ten** international joint investigation teams³² (JITs) related to the investigation of international **money laundering crimes**. In **four** of the JITs, the money laundering crime was prosecuted in Estonia, while in six cases, the money laundering crime occurred in another country. Participation in international investigation teams confirms that the Estonian financial system is used in international money laundering schemes.

Table 6. Participants in JIT proceedings with Estonia

Country	Number of participations in JITs
Latvia	3
Ukraine	3
Finland	2
Sweden, Denmark, Switzerland, Lithuania, Romania, France	1

Source: Prosecutor's Office

³² Joint Investigation Team or JIT.

According to data from foreign inquiries³³ received between 2020 and 2024, money laundering proceedings conducted in other countries are mainly related to Estonia through **layering activities**, where the bank accounts of companies located in Estonia are often used.

International cooperation in preventing money laundering during the observed period was similar to the previous national risk assessment period, with about twice as many inquiries and information transmissions received by the FIU compared to those sent out from Estonia. Generally, the most communication occurred with neighboring countries. In 2022, Malta emerged as an active foreign inquiry maker, not indicating a higher risk level but resulting from additional resources given to the Malta Financial Intelligence Analysis Unit and increased capacity to focus on crimes committed through Malta. It was confirmed that money laundering is a cross-border crime and information exchange is extremely important.

Fraud committed abroad remains the most common predicate offense. International fraud cases involving Estonian victims have increased. During the observed period, inquiries were also received from other areas, such as drug trafficking and organized crime. In 2024, the number of foreign inquiries related to tax crimes and cash transactions increased compared to previous years.

In 2023–2024, money laundering-related inquiries were largely related to cash, while less attention was paid to payment instruments. In 2024, the number of foreign inquiries related to cash transactions received by the FIU and the number of cash reports submitted by market participants increased significantly. Since 2021, the volume of cross-border cash transactions entering Estonia has been almost four times greater than those leaving Estonia. Between 2020 and 2024, the number of cash declarations increased by 67%, and the declared amounts increased each year. While over €12 million in cash was declared in 2020, this amount exceeded €320 million in 2024. The number of declarations by legal entities remained stable, while the number of declarations by individuals increased by 87%.

According to the FIU, the level of money laundering risk associated with cash remains high, especially in the service sector, where cash is widely used. The increase in large cash transactions has raised the risk level of several such services. Systematic and large-scale cash movements may indicate links to economic crime or other organized crime, making it a significant warning signal from a money laundering perspective.

Since 2021, the amounts of cross-border transactions reflected in the FIU's information have increased significantly. The most important **destination countries for suspicious money**, based on transaction amounts in reports, were Lithuania, the United Kingdom, Poland, Bulgaria, and Switzerland. The most important **departure countries** were Lithuania, Germany, Latvia, Finland, the United Kingdom, and Poland. The FIU frequently received information about suspicious transactions by Estonian individuals that took place in payment accounts opened at foreign banks and e-money institutions. In terms of transaction volumes on foreign accounts used by Estonian individuals, the standout countries were Lithuania, Belgium, Malta, the United Kingdom, Austria (debit transfers), and Germany (credit transfers)³⁴.

Between 2020 and 2024, the most foreign inquiries to Estonian investigative authorities came from Latvia, Poland, Finland, and Germany, accounting for 60% of all inquiries. The FIU received the most inquiries from Malta (13% over the years), Germany (12%), Latvia (10%), Finland (8%), and Lithuania (8%). Between 2020 and 2022, the main inquirers were the financial intelligence units of Germany, Finland, and Latvia. The most cross-border potential money laundering reports were received by Estonia from the Netherlands, Italy, Latvia, and Germany. The incoming inquiries to the PBGB involved 55 different criminal compositions, as shown in Table 7.

³³ According to the Estonian FIU data.

³⁴ FIU Yearbook 2024, p 25.

Table 7. Types of Crimes Mentioned in Incoming Inquiries to the PBGB

Type of Crime	Share of Incoming Inquiries
Fraud	26%
Tax Evasion	14%
Computer Fraud	8%
Drug Trafficking	6%
Embezzlement	5%

Source: PBGB

Between 2020 and 2024, investigative authorities sent inquiries mainly to Lithuania, Latvia, Germany, the USA, Finland, Spain, the Netherlands, Russia, and the United Kingdom; the total number of inquiries accounted for 63%. Over the years, Lithuania has been the main target country in terms of share. The number of inquiries sent to Latvia and Germany has decreased. Most legal assistance requests with a money laundering qualification were sent to **Lithuania, Ireland**, Spain, the USA, and Germany.

Table 8. Main target countries for FIU inquiries between 2020 and 2024

Country	Share of Inquiries
Lithuania	13%
UK	6%
Germany	6%
Latvia	6%
Finland	5%

Source: FIU

Table 9. Criminal Compositions of Inquiries Sent Out by the PBGB Between 2020 and 2024

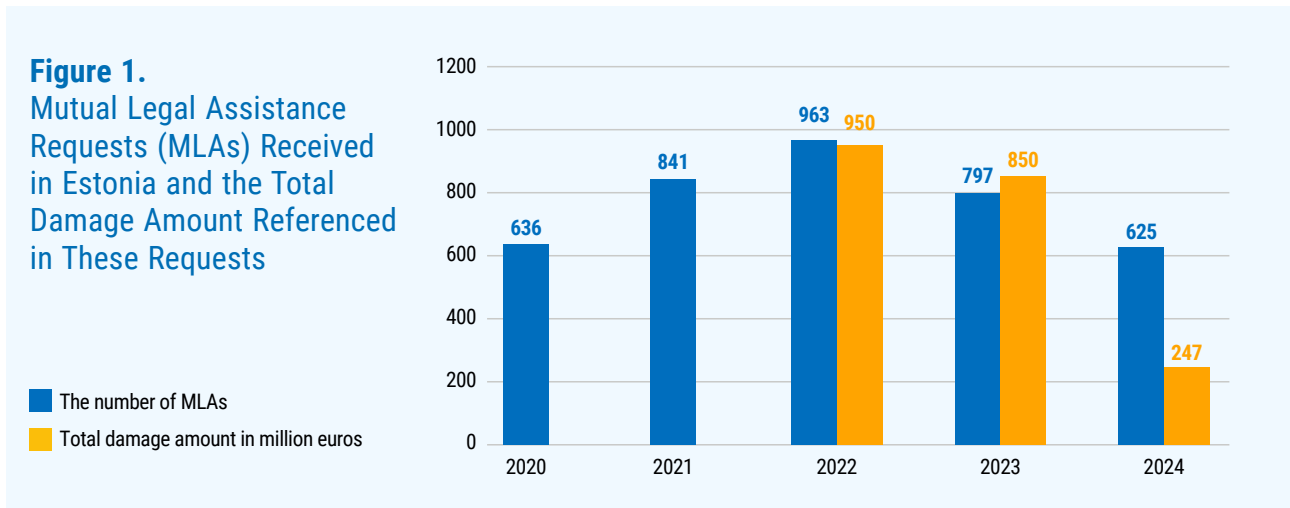
Type of Crime	Share of Inquiries
Computer Crimes	53%
Fraud	8%
Investment Fraud	6%
Unauthorized or Prohibited Economic Activity	5%
Other	28%

Source: PBGB

Based on information received from foreign countries, it can be said that companies registered in Estonia have predominantly been used to commit crimes, including tax offenses, elsewhere in the world³⁵. Generally, these companies have a weak connection to Estonia – they do not have a permanent establishment in Estonia, or

³⁵ The cases are described in Chapter 7 on the exploitation of legal entities.

the company is backed by e-residents or foreign nationals who do not reside in Estonia. It should be noted that the situation depicted by foreign inquiries is subject to a delay – by the time the inquiry is made, the company’s license may be invalid or in the process of being revoked. It can be expected that this trend will continue in the future.



In recent years, the use of virtual IBAN accounts (**VIBANs**³⁶) for moving and laundering criminal proceeds obtained through fraud has increased. Although this trend continues, data from 2024 indicates a slight decrease in this usage. A problem in investigating crimes related to VIBANs and responding to legal assistance requests has been that the VIBAN service provider, who intermediates the service to various payment intermediaries, cannot assume the responsibility for responding, as investigative authorities lack access to the necessary data for the proceedings. Fraud committed abroad is decreasing, and information from foreign countries points to fraud involving Estonian individuals on e-commerce platforms. International fraud cases involving Estonian victims have increased, and domestic fraud has become more systematic and organized.

Among the clients of banks operating in Estonia, 147 legal assistance requests (23.5%) were received in 2024 regarding payment intermediaries, which is numerically less than the previous year, when 304 cases (38%) were registered. At the same time, the total damage amounts caused by crimes have increased: while in 2023 the total damage reflected in legal assistance requests amounted to 133 million euros, in 2024 the total damage reached 150 million euros. This indicates that the **money laundering risk associated with payment intermediaries using correspondent services remains high.**

³⁶ VIBAN (Virtual International Bank Account Number) is not a separate account from the perspective of a credit institution, but rather a technical account for the payment service provider.

3. National ML Vulnerability

3.1. Description of the Methodology

National vulnerability indicates the existing protection and response mechanisms for preventing money laundering. National vulnerability is influenced by the vulnerabilities of various sectors that may be exploited for money laundering. The World Bank assessment module³⁷ is used to measure national money laundering vulnerability.

The national vulnerability module includes 22 assessment criteria. Based on these criteria, the effectiveness of the national anti-money laundering system can be assessed and measured:

- The quality of anti-money laundering policies and strategies
- The effectiveness of the definition of money laundering offenses
- The scope of asset confiscation laws
- The quality of information collection and processing by the FIU
- The capability and resources for investigating financial crimes (including asset confiscation)
- The integrity and independence of financial crime investigators (including asset confiscation)
- The capability and resources for prosecuting financial crimes (including asset confiscation)
- The integrity and independence of financial crime prosecutors (including asset confiscation)
- The capability and resources of court processes (including asset confiscation)
- The integrity and independence of judges (including asset confiscation)
- The quality of border controls
- The thoroughness of customs controls regarding cash and similar instruments
- The effectiveness of customs controls regarding cash and similar instruments
- The effectiveness of national-level cooperation
- The effectiveness of international cooperation
- The level of economic formalization
- The level of financial reliability
- The effectiveness of tax compliance
- The availability of independent audits
- The availability of reliable identification infrastructure
- The availability of independent information sources
- Access to and availability of beneficial ownership information

Qualitative and quantitative data were used in the assessments based on the listed criteria: the experience and opinions of the working group experts, criminal statistics, court decisions on money laundering cases, statistics on the procedures and information exchange of supervisory and law enforcement agencies, statistics on incoming and outgoing international inquiries and legal assistance requests, and statistics on asset seizure and confiscation, as well as statistics on the personnel of the institutions, etc.

³⁷ World Bank assessment module „Module 2 National Vulnerability“.

3.2. National Vulnerabilities of the AML System

Successful prevention of money laundering requires the state to have a good understanding of its risks, including vulnerabilities. Estonia is digitally advanced and strongly connected to the international economy. Such an environment offers many advantages but also brings risks – for example, criminals may use complex technological solutions to conceal their activities. For the anti-money laundering system to be effective, Estonia must be able to detect risks early and address them purposefully.

This chapter describes the main national vulnerabilities that may hinder the prevention of money laundering. It also analyzes how laws, supervisory authorities, and cooperation between various parties function. Understanding vulnerabilities is an important step in making informed decisions and strengthening Estonia's ability to combat money laundering.

General National Vulnerability

Estonia's overall national money laundering vulnerability score is **medium**, consisting of the composite score³⁸ of 21 national vulnerability criteria and the composite score³⁹ of 19 sectoral vulnerabilities.

The overall vulnerability score was supported by effective cooperation both domestically and internationally, as well as a reliable identification infrastructure and the collection and processing of financial information by the FIU and the Financial Supervision Authority. The assessment was negatively affected by the lack of real-time statistics and a national strategy, as well as gaps in the legal framework for asset seizure and confiscation and the reliability of the beneficial ownership register data. Investigative authorities should review priorities in resource allocation to ensure sufficient capacity to detect and investigate money laundering and criminal proceeds.

3.2.1. Investigation of economic crimes: resources and capabilities

In Estonia, several agencies are involved in the prevention, detection, and combating of economic crimes, including the Police and Border Guard Board (PBGB), the Tax and Customs Board (TCB), the FIU, the Financial Supervision Authority (FSA), the Internal Security Service (ISS), the Prosecutor's Office, and the Environmental Board.

According to the assessment of the resources and capabilities of state institutions, Estonia has **above medium** level of vulnerability. The main reason for this assessment is that without sufficient human resources in the fight against economic crime, the existing legal framework, tools, cooperation networks, and best practices have limited impact. Effective prevention of money laundering requires not only systems but also adequate human resources.

a) Police and Border Guard Board

At the PBGB, criminal cases are investigated by the criminal bureaus of the prefectures and the central criminal police. During the period under review, the total number of investigators was 370 officers, of whom about 65 were engaged in the fight against economic crime. The personnel remained at a similar level during the period under review. There was no specialized unit for financial crimes; these crimes were investigated by the same investigators along with other crimes.

³⁸ Medium vulnerability.

³⁹ Medium vulnerability.

The identification and seizure/confiscation of criminal proceeds are crucial parts of criminal proceedings as they hinder the capabilities of criminals and have a preventive effect. In the investigation of serious hidden crimes, financial investigations are conducted in parallel to assess the existence and extent of assets subject to confiscation. The Central Criminal Police has a separate bureau for identifying criminal proceeds (17 officers) and investigators specialized in identifying criminal proceeds in the prefectures (4 officers).

The unit supporting the investigation of financial crimes is the Criminal Intelligence Analysis Department (KRAT) located in the Central Criminal Police, where 6 officers support the field of so-called white-collar crime⁴⁰ and 5 officers support the field of organized and cybercrime. KRAT also includes a liaison officer between the PBGB and the FIU, whose main task is to facilitate information exchange between the PBGB and the FIU. KRAT also contributes to the creation and development of analytical tools, which are an important part of preventing and investigating financial crimes.

On a positive note, in 2023, the PBGB received 10 additional positions to enhance the capacity for investigating white-collar crime (including financial crimes) – the Eastern and Southern prefectures each received 4 positions, and the Northern prefecture received 2 positions. These positions enabled the creation of cyber and economic crime investigation groups in the Eastern and Southern prefectures, which established the capacity to investigate financial crimes. In the Northern prefecture, the positions were added to the existing staff, allowing resources to be freed up for the investigation of money laundering crimes. While the relevant officers in the Eastern prefecture are still gaining experience, the officers in the Southern prefecture are already capable of substantively investigating financial and money laundering crimes. The level of vulnerability is increased by the fact that, until now, a large part of the human resources has been spent on investigating predicate offenses, mostly fraud.

In 2021, the PBGB introduced a handbook for investigating money laundering crimes. The purpose of the handbook is to provide investigators dealing with money laundering crimes with a helpful tool that gives an overview of the elements of money laundering both internationally and in Estonian law, as well as the regulations and case law related to asset seizure and confiscation, which should be considered in both pre-trial and trial proceedings. The handbook also provides an overview of how to enhance and expedite international cooperation in the investigation of money laundering crimes. The handbook is for internal use and is available to investigators via the PBGB intranet.

PBGB officers have the opportunity to improve their knowledge and skills in money laundering through both national and international training. During the period under review, a positive trend can be noted in the increase in both the number of training sessions and the number of participants. For example, while there were a total of 3 training sessions with 15 participants in 2020, there were already 14 training sessions with 127 participants in 2024.

The impact of the lack of necessary tools during the reporting period is not significant. On a positive note, the PBGB has an up-to-date cryptocurrency analysis tool.

The number of registered money laundering crimes and proceedings in the PBGB remained at the same level during the period under review, but an increase can be observed in 2024 compared to 2023. The main increase came from the proceedings of the Central Criminal Police. The investigation of money laundering as a serious hidden crime is time-consuming, and therefore the number of registered cases is not proportionally large. Based on the fluctuations over the years, no definitive conclusions can be drawn, but a positive impact can be noted in that the prevention of money laundering was a higher priority in the Estonian investigative and supervisory authorities during the period under review, which helped to keep the number of crimes stable.

⁴⁰ Economic, corruption, and money laundering crimes.

Table 10. Registered money laundering crimes (Penal Code § 394) by year of registration and by the investigating sub-agency/unit

Sub-agency/unit	2020	2021	2022	2023	2024	Total
Central Criminal Police	6	13	8	2	10	39
Eastern Prefecture	1	1	0	2	0	4
Southern Prefecture	0	0	0	0	1	1
Western Prefecture	0	1	0	0	0	1
Northern Prefecture	5	6	8	6	7	32
Total	12	21	16	10	18	77

Source: PBGB

Table 11. Number of criminal cases in which at least one money laundering crime (Penal Code § 394) was registered in the respective year by the investigating sub-agency/unit

Sub-agency/unit	2020	2021	2022	2023	2024	Total
Central Criminal Police	6	8	5	2	9	30
Eastern Prefecture	1	2	0	2	0	5
Southern Prefecture	0	0	0	0	1	1
Western Prefecture	0	1	0	0	0	1
Northern Prefecture	6	5	7	4	5	27
Total	13	16	12	8	15	64

Source: PBGB

b) Prosecutor's Office

The investigation and prosecution of financial crimes were one of the priorities of the prosecutor's office during the period under review. The importance of this field, both at the national level and from the perspective of the prosecutor's office, is confirmed by the structural reforms implemented in the prosecutor's office in recent years. As a result, in November 2023, the Prosecutor General's Office established a special prosecution department 2 (hereinafter "SO 2")⁴¹ focused on the investigation of economic and corruption crimes. SO 2 consists of a chief state prosecutor, six state prosecutors, three assistant prosecutors, and two consultants. Additionally, on March 1, 2024, the District Prosecutor's Office for Economic and Corruption Crimes (hereinafter "MARP") was established, focusing on the investigation of financial crimes. MARP's staff includes 37 prosecutors (assistant prosecutors, district prosecutors, three senior prosecutors, a chief prosecutor) and six consultants, including three special consultants (specializing in financial crimes, money laundering, and criminal proceeds). Considering that there are 185 prosecutor positions in the Republic of Estonia and that 47 prosecutors are specialized in combating financial crimes, it can be concluded that about 25% of the prosecutors in the prosecutor's office are dedicated to investigating economic crimes such as money laundering.

However, in assessing national vulnerability, it should be taken into account that as of the end of 2024, the MARP prosecutors specialized in money laundering are handling nine money laundering criminal cases. Considering that extensive international cooperation and the submission of seizure applications to the court are required in

⁴¹ The responsibility also includes performing the prosecution function in cross-border or high-public-interest economic crimes (including money laundering).

all criminal cases, these prosecutors cannot currently take on new cases. Although the PBGB's resources have been increased (ten additional positions) in recent years, the number of prosecutors has remained the same.

The lack of resources in the prosecutor's office is indicated by the absence of prosecutors specialized in asset seizure and confiscation. Both the prosecutor's office and the Ministry of the Interior have consistently emphasized the need for additional resources to establish a separate unit for asset seizure and confiscation in the prosecutor's office, but these proposals have so far been unsuccessful. Establishing a separate unit for asset seizure and confiscation would significantly enhance the prosecutor's office's capacity in this area and increase the ability to impact criminals' assets. After all, the primary motive for committing crimes, especially financial crimes, is criminal proceeds, and to ensure that crime does not pay, the proceeds must be taken away from the perpetrators.

This fact is also confirmed by recent criminal statistics (see Table 12). According to these statistics, the volumes of asset seizure and confiscation have remained at a similar level during the period under review.

Table 12. Number of criminal cases vs. value of seized assets

	2020		2021		2022		2023	
	Number of criminal	Value of confiscated assets, eur	Number of criminal	Value of confiscated assets, eur	Number of criminal	Value of confiscated assets, eur	Number of criminal	Value of confiscated assets, eur
Southern District	27	311,180	19	22,615	12	109,397	15	333,440
Western District	28	42,333	24	78,751	23	48,408	14	88,601
Northern District	158	706,931	113	438,928	142	322,151	127	1,659,048
Viru District	29	354,254	25	161,759	23	252,072	21	148,162
Prosecutor General's Office	7	821,804	9	663,566	8	1,665,535	6	202,153
Total	249	2,236,503	190	1,365,619	208	2,387,563	183	2,431,403

Source: Prosecutor's Office

During the period under review, the challenges identified include the complexity of detecting predicate offenses for money laundering (especially autonomous money laundering). Predicate offenses related to money laundering are mostly committed outside Estonia, and their detection requires very close and rapid international cooperation. Whether it is possible to detect and prove the predicate offense at all depends largely on the willingness of other countries to cooperate. Unfortunately, it must also be considered that substantial cooperation with some countries is practically non-existent.

International cooperation is also necessary to identify the object of money laundering that has moved outside Estonia and the existence of criminal proceeds located in foreign countries. One vulnerability in this regard is that, unlike Estonia, many countries do not have central registers (e.g., for beneficial owners and real estate), making it difficult to quickly identify the existence of assets located outside Estonia.

Prosecutors participate in internal and external training sessions every year. Prosecutors are trained in both asset seizure and confiscation and money laundering. The prosecutor's office has established a training council that plans the institution's training activities and decides on the organization of specific training sessions. Considering that separate units have been created in the prosecutor's office to combat financial crime, where specialized prosecutors work and are provided with field-specific training, it can be concluded that prosecutors have the competence to combat financial crimes (including money laundering). One prosecutor from the MARP team handles money laundering criminal cases full-time, and other prosecutors also deal with other economic and corruption crimes, so several prosecutors have experience in investigating money laundering and representing the state in this type of crime. SO 2 prosecutors also have experience in investigating and prosecuting money laundering. Similar to the PBGB, the 2021 handbook for investigating money laundering crimes is used in daily work.

Prosecutors have comprehensive access to the necessary information and documents. All prosecutors have access to the data collections required for their daily work, and the law guarantees prosecutors the right to request information (Code of Criminal Procedure § 215 (1) and § 32 (2)).

c) Tax and Customs Board

The Investigation Department of the Tax and Customs Board (TCB) employs about one hundred investigators who handle tax and customs crimes as well as cross-border drug crimes. The TCB can investigate money laundering with the prosecutor's permission in cases where the predicate offense or perpetrators are under the TCB's jurisdiction. Typically, the PBGB has the authority to investigate money laundering from tax crimes committed in another country, and they can also investigate tax crimes when necessary, which was done on several occasions during the period under review.

From 2020 to 2024, the TCB initiated proceedings in two money laundering cases. In investigating tax crimes, the TCB focuses on a specific time period and proving tax evasion within that period, as well as finding and seizing assets to cover the tax claim, which is a public-law claim. Typically, the money involved in the investigated tax crimes is the money saved by avoiding tax obligations, which allows the taxpayer to offer services or products at a lower price than competitors, and the state usually has an obligation to ensure payment upon submission of a public-law claim. In such cases, no criminal proceeds are generated, and no money laundering follows.

In rare cases where the perpetrator has made an unjustified refund claim or concealed money taken out of an insolvent taxpayer, it is difficult to distinguish between tax crime and self-laundering. Additional resources for proving the latter are generally avoided, considering the potential outcome. Criminal proceedings conducted by the TCB's Investigation Department usually involve financial investigations, as the department's goal is to identify the exact tax damage, assets to be seized to cover the tax claim, and/or criminal proceeds. Extensive financial investigations are not conducted in low-priority drug crime cases, but they are certainly involved in cases of cross-border drug smuggling groups. Financial investigations are conducted by criminal investigators who mostly have higher education in police or tax matters but have not usually undergone separate training in financial investigations. The department has seven investigators specialized in identifying criminal proceeds, who are distributed among the sub-units handling the proceedings and should primarily support the identification of assets obtained through crime and/or to be seized in priority proceedings.

A factor increasing the level of vulnerability is the uneven preparation of investigators, which in some cases is limited to instructions received from colleagues rather than systematic and continuous training. During the period under review, there were cases where the identification of assets located abroad was not carried out due to slow international cooperation or a lack of resources in the prosecutor's office and courts.

d) Internal Security Service

The task of the Internal Security Service (ISS) is to ensure national internal security through information

gathering and the use of preventive measures, as well as the investigation of offenses to the extent established by a regulation of the Government of the Republic. The regulation also sets out ISS's mandate for investigating money laundering crimes.

ISS does not have a separate structural unit for investigating financial crimes or money laundering. Investigators who deal with money laundering crimes also handle asset confiscation and seizure as needed during the proceedings. Capabilities are developed through investigations, and experienced investigators have been retained on the job.

Investigators are provided with the necessary knowledge for preventing money laundering and terrorist financing and have opportunities to improve their skills. During the period under review, ISS received training from both national (e.g., the Academy of Security Sciences, FIU) and international partners (e.g., CEPOL). Additionally, experiences are exchanged through bilateral contacts with partner services in Europe.

During the period under review, ISS found evidence of money laundering in two criminal cases⁴² under investigation (both money laundering under Penal Code § 394 and money laundering agreement under Penal Code § 394¹). In one criminal case, assets worth €98,250.17 were seized.

Considering the increased security threats arising from global crises (including the COVID-19 pandemic) and Russia's war in Ukraine, as well as the rapid technological developments in encrypted communications and financial technology payment solutions, the agency's current resources are limited.

e) Environmental Board

The Environmental Board is responsible for detecting and investigating environmental offenses, which is handled by the supervision field consisting of six regional offices and an investigation department. In total, approximately 120 inspectors are involved in environmental supervision, and the investigation department has ten investigators, five of whom primarily deal with more serious misdemeanors and five with crimes. During the period under review, the Environmental Board did not investigate or identify any money laundering cases, which should be considered a factor increasing national vulnerability. The Environmental Board focuses primarily on identifying and recovering environmental damage. Since environmental crimes stipulated in the Penal Code⁴³ can also be predicate offenses for money laundering, and the FIU's reports from 2020-2024 have included cases where assets obtained through environmental crimes were suspected of being linked to money laundering, the absence of such investigations by the KeA indicates limited capacity to handle money laundering cases.

The Environmental Board lacks the authority to conduct surveillance operations, which also limits its ability to investigate these crimes. There are also significant shortcomings in extended confiscation. Since it is not possible to apply extended confiscation under Penal Code § 83-2 to perpetrators of environmental crimes (ordinary confiscation and seizure are possible), and since no environmental crime allows for extended confiscation, this means that one lever for controlling professional environmental criminals is missing.

f) FIU

The Financial Intelligence Unit (FIU) has been operating as a separate government agency under the Ministry of Finance in Estonia since 2021, which has increased both the agency's independence and autonomy in fulfilling its core tasks. The effectiveness of the FIU in collecting, analyzing, and transmitting information related to money laundering to investigative authorities is rated as good. Increased financial and human resources, in addition to strengthening case-specific analysis, have enabled the creation of the FIU's strategic analysis department and a unit dealing with data management to ensure the identification and systematic monitoring of money laundering risks, threats, patterns, and methods across sectors.

⁴² There have not yet been any convictions in either of the criminal cases.

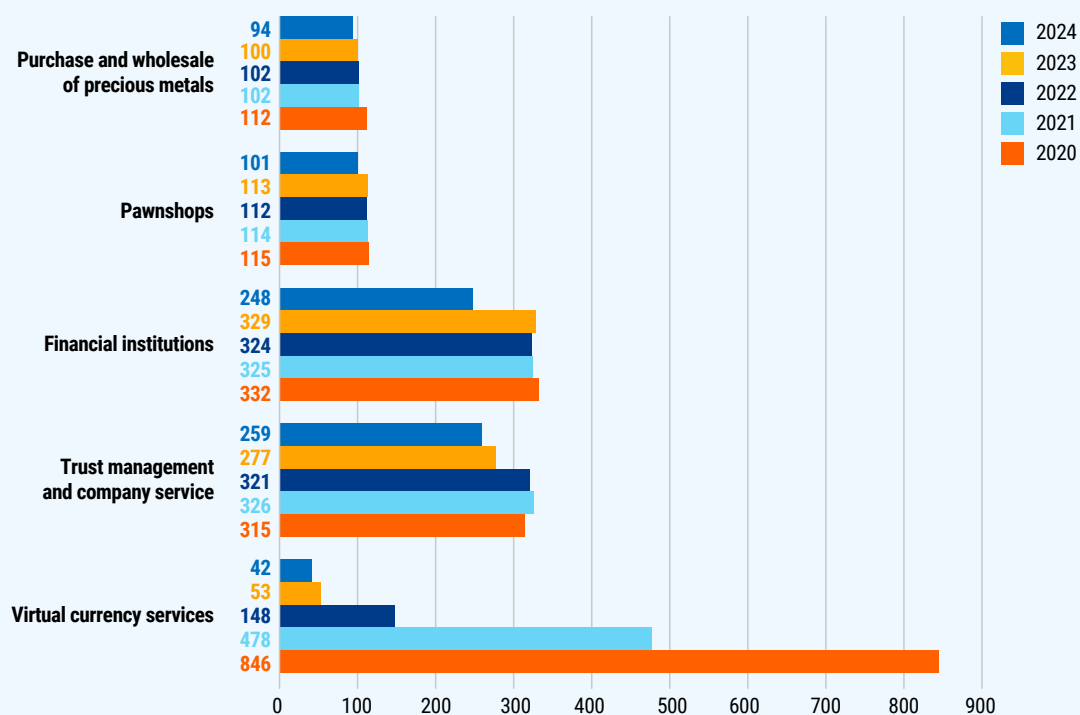
⁴³ Chapter 20th of the Penal Code.

The FIU conducts national supervision over obligated entities under § 54(1)(4) and § 54(1)(9) and § 64(1) of the MLTFPA and issues activity licenses under § 70-75 of the MLTFPA. In 2023, the FIU received additional resources for this area, which was essential to ensure the necessary average level of capacity for the work.

In supervision, the principle of risk-based supervision is to focus and direct more resources to those sectors where the risk level of money laundering and terrorist financing and evasion of financial sanctions is higher. During the period under review, the focus of supervisory proceedings was on virtual currency service providers, trust and company service providers, and financial institutions.

As a result of the FIU's work, the number of activity licenses in high-risk sectors, such as virtual currency services, trust management, and company services, has decreased. Additionally, the financial institutions sector has been streamlined. In recent years, the public has clearly seen how previously taken risks in the virtual currency service provider sector have accumulated and eventually materialized. This has also been the reason why the FIU has had to allocate a significant portion of its resources to this area.

Figure 2. Number of activity licenses issued by the FIU by year as of the end of the year.



Source: FIU

Although the FIU follows a risk-based approach in supervision, identified deficiencies indicate that it is not always sufficiently effective. More resources should be directed to on-site inspections, which cannot replace remote inspections. In several sectors (real estate and precious metals sector, company service providers, lawyers), a lack of awareness of money laundering risks and due diligence obligations has been identified, requiring targeted training and guidance. The division of supervision (e.g., between the TCB and the FIU in the gambling sector) and difficulties in communicating with foreign companies (lack of a contact person requirement) indicate that cooperation and information exchange need to be improved. In many professional and freelance sectors (e.g., bailiffs, bankruptcy trustees, accountants, tax advisors), the problem is the shortage of human resources in the FIU, meaning that the number of employees has not been

sufficient to ensure effective supervision and analytical capacity in these sectors. This limits the ability to provide on-site inspections and specific guidelines. Due to limited resources, the FIU has had to narrow its focus, leaving other vulnerable sectors under insufficient supervision.

The FIU has good capabilities to transmit information and its analysis results to relevant competent authorities both upon request and spontaneously. The FIU has the ability to detect cross-border activities.

The FIU provides analyzed or fact-based information to investigative authorities, which is entered into the POLIS information system. Investigative authorities use this information to initiate and conduct ongoing criminal proceedings. Most of the fact-based information pertains to predicate offenses related to money laundering, and to a lesser extent, information related to suspected money laundering. This information supports investigative authorities in detecting and preventing crimes.

In 2024, the transmission of fact-based information to investigative authorities through the POLIS information system increased significantly. Investigative authorities initiated 10 criminal proceedings in 2024 and 11 in 2023 based on the analyzed transmissions from FIU, which are related to money laundering or its predicate offenses. Additionally, larger analysis projects have been carried out between FIU and the PBGB, where a significant amount of report data was used. The situational awareness derived from these analyses has been utilized by PBGB in their information gathering, analyses, and planning of criminal proceedings.

Table 13. Number of reports submitted by FIU to investigative authorities by year and type of report

Type of report	Number of reports ⁴⁴				
	2020	2021	2022	2023	2024
STR	199	259	81	93	689
UAR/UTR	361	112	67	46	467
Total	560	371	148	139	1,156 ⁴⁵

Source: FIU

When a separate strategic analysis department was established within the FIU in 2021, the capability to analyze reports on a strategic level and use this knowledge in various products shared internally and with investigative authorities increased significantly. Since December 2022, the FIU has been publishing typology reports to help sectors better plan their activities based on risk, thereby improving the quality of reporting. The purpose of the typology report is to provide the market or a specific sector with guidelines to recognize threats using described indicators and to be more proactive in identifying new potential criminal patterns.

IT solutions are being developed (e.g., automatic pre-analysis, data warehouse, enhanced data processing capabilities, network analysis, OCR⁴⁶) to increase the FIU's ability to identify new threat patterns and detect typologies of anomalies and suspicions.

The FIU's budget and human resources have increased in recent years, which has certainly contributed to the agency's capabilities. However, a vulnerability is the lack of guaranteed permanent funding for IT system

⁴⁴ Does not include the number of reports used in the products of the strategic analysis department that were forwarded to investigative authorities.

⁴⁵ In 2024, the transmission of fact-based information to investigative authorities through the POLIS information system increased significantly – a total of 748 reports were entered.

⁴⁶ Text recognition.

development and certain fixed costs. When the FIU was transferred to a separate government agency, the necessary permanent funding for IT investments was not secured, and the FIU has used budget surpluses from 2021–2023 for this purpose, which are now being exhausted. Additionally, the FIU is implementing the EU-funded SAF project (Strategic Analysis Function), which lacks guaranteed permanent funding. If permanent funding is not secured, it will significantly impact the FIU's capabilities and development from 2027 onwards, as the FIU will have to find money from its budget to cover costs.

The FIU has a reporting portal where obligated entities (e.g., banks, payment service providers) submit suspicion-based (STR, UAR/UTR)⁴⁷ and threshold-based (CTR) reports. By 2026, a new reporting portal will be developed to improve the quality and convenience of report submissions and provide better feedback. The portal will also enhance the FIU's analytical capabilities by offering more opportunities for automation.

During the observed period, the FIU improved the awareness of obligated entities and increased the quality of reports through training, information sessions, feedback reports, and typology reports. However, the reporting activity and quality of reports from some sectors remain low.

g) Financial Supervision Authority

The Financial Supervision Authority has significantly enhanced its AML supervision capabilities during the assessment period by increasing human resources, improving supervisory processes, and developing technical solutions. The FSA has adopted additional technological capabilities in supervision and strengthened cooperation with local market participants through the public and private sector cooperation forum, as well as internationally through AML supervisory colleges and the Nordic-Baltic cooperation forum.

To measure money laundering risks, the FSA introduced a risk dashboard⁴⁸ in 2020, which helps identify and assess the risks of money laundering and financial sanctions evasion in the activities of financial supervision subjects and take necessary measures to mitigate these risks. The risk indicators of the dashboard are based on the opinion of the European Banking Authority, the EU-wide risk assessment published by the European Commission (SNRA), the national risk assessment of Estonia (NRA), information received from the FIU, law enforcement agencies, and intelligence services, as well as feedback received during the 2022 MONEYVAL evaluation.

Initially, the risk dashboard measured risks related to payments and deposits of credit institutions. In 2023, it was also developed for payment institutions and e-money institutions, and by the end of 2024, for investment firms. At the beginning of the full-scale military conflict between Russia and Ukraine, an additional risk dashboard was created to monitor changes related to Russia or Belarus that could potentially affect the Estonian financial system.

Based on the results of the risk dashboard, the FSA has conducted ad hoc checks and/or inquiries on financial supervision subjects, planned full-scope inspections and/or thematic or targeted inspections. A summary based on the risk dashboard is compiled at least twice a year, providing an overview of indicator values and general new trends. Risk dashboard memorandums are regularly shared with the FIU. Memorandums are not shared with market participants.

The improved efficiency of the FSA's supervision and the special attention paid to cross-border risks is also reflected in the strengthening of international cooperation within the framework of AML supervisory colleges. During the assessment period, the FSA has established supervisory colleges for five financial institutions registered in Estonia and contributes to the work of 14 AML supervisory colleges established by supervisory authorities of other countries.

⁴⁷ More detailed explanation in "Abbreviations".

⁴⁸ <https://www.fi.ee/et/uudised/finantsinspeksioon-votab-kasutusele-uee-rahapesu-riskide-mootmise-masina>

h) Court Proceedings

In Estonia, there are no judges specialized in handling money laundering crimes or confiscations. The distribution of judges' work is determined by the annual work plan of the county court, which is publicly available on the courts' website⁴⁹. Generally, the court proceedings for money laundering criminal cases can be considered satisfactory. Most criminal cases sent to court are in plea bargaining procedures, where efficiency and processing time are adequate. However, the problem lies with criminal cases resolved in general proceedings, where processing times can be long, often leading to the termination of court proceedings in complex criminal cases due to either the expiration of the statute of limitations or the passing of a reasonable time limit for proceedings.

Table 14. Average processing time of economic crime criminal cases in general proceedings by year of resolution (Penal Code § 201 (2) 3, § 209 (2) 2, § 213 (2) 2, §§ 294–300¹, §§ 402¹, 402³, and 402⁴)

Year	Number of Resolved Proceedings	Average Processing Time	Median	Longest Proceeding	Shortest Proceeding
2024	10	773	521	2,464	251
2023	9	637	500	1,440	133
2022	10	386	345	819	40
2021	8	546	469	1,372	49
2020	14	381	289	1,200	16

Source: Prosecutor's Office

Table 15. Average processing time of criminal cases with money laundering offenses in general proceedings by year of resolution

Year	Number of Resolved Proceedings	Average Processing Time	Median	Longest Proceeding	Shortest Proceeding
2024	3	1,288	975	2,464	424
2023	3	862	865	1,221	500
2022	4	516	588	819	67
2021	3	396	190	950	49
2020	8	471	313	1,200	16

Source: Prosecutor's Office

The average processing time for criminal cases involving money laundering offenses has increased more rapidly than for economic crime cases in general. This indicates the growing complexity and increasing resource requirements for handling money laundering criminal cases, as the number of criminal cases sent to court continues to rise.

⁴⁹ <https://www.kohus.ee/dokumendid-ja-vormid/kohtute-toojaotusplaanid>

Table 16. All decisions related to § 394 by year of entry into force

Year	2020	2021	2022	2023	2024
Criminal cases sent to court	12	7	8	5	5
Convictions	10	5	4	4	3
Natural persons	17	13	9	14	4
Legal persons	2	0	0	0	0
Acquittals	3	1	2	0	1
Natural persons	5	2	4	0	2
Legal persons	4	0	1	0	0

Source: Prosecutor's Office

The general awareness of judges regarding the specifics of the money laundering field is low, and during the observed period, there were not enough training sessions to help improve the situation.

i) Border and Customs Controls

The overall assessment of the capacity of border and customs controls is good. Estonia has only one non-EU neighboring country, separated by natural barriers such as the Narva River, Lake Peipus, Lake Lämmijärv, and forest areas. A border infrastructure is being built along the land border to prevent the free movement of people, which Russia is currently partially duplicating, making the prevention of illegal border crossings even more effective in the future. At official border points, the PBGB and the TCB work closely together in controlling individuals crossing the border. Free movement of people and goods occurs between EU countries according to Schengen rules, and to prevent malicious exploitation, the PBGB and TCB conduct random checks near border crossing points. The implementation of these checks increased the number of cash declarations by travelers entering and leaving from third countries during the observed period, indicating a strong system, but there is still a need to address some identified weaknesses.

From 2020 to 2024, Estonia's border and customs control system has shown strong capability in mitigating money laundering risks, but there are also areas that need additional attention. The TCB applies EU and national legislation that allows effective supervision of cash and precious stones moving across the border. Customs have access to modern technical equipment and cash detection dogs, and officers regularly participate in training, which also includes techniques for detecting hidden cash. Customs actively cooperate with international partners, participating in joint operations and sharing risk information.

The Cash Declaration System (SDS) and the FIU's information system (RABIS) exchange data in real-time, but the FIU lacks the capacity to fully process this data, which may hinder the rapid detection of false declarations. However, the TCB did not identify any cases of false cash declarations from 2020 to 2024.

The additional tasks related to sanctions supervision due to Russia's war of aggression in Ukraine have not received additional resources, which may affect the overall effectiveness of supervision. To mitigate sanction risks, the TCB switched to full customs control⁵⁰ for exports from August 8, 2024. Lenient penalties⁵¹ and the failure to confiscate cash may reduce the risk perception of offenders, especially in cases of sanctioned euros being taken out in cash on the outbound route.

⁵⁰ TCB's Yearbook [Maksu- ja Tolliamet](#) aastaraamat | [Maksu- ja Tolliamet](#)

⁵¹ Administrative fine up to €2400.

To reduce the level of vulnerability, legislation has been amended so that, as of April 27, 2025, the TCB is required to handle violations related to the import and export of sanctioned goods and cash. A positive development is the doubling⁵² of the fine unit rate under § 47 of the Penal Code. The failure to confiscate cash does not have a sufficient deterrent effect, especially in cases of cash violations detected on the outbound route.

Border crossers can find information about the obligation to declare cash and other items on the TCB's website⁵³ and at border points. Information leaflets, posters, and screens are used at border points, and border crossers are verbally asked if they have any items to declare.

During the COVID-19 pandemic, the number of border crossings decreased, leading to a temporary decline in the number of cash declarations. Since the beginning of the war in Ukraine, the number of cash violations related to evading sanctions has increased, especially on the outbound route.

3.2.2. Seizure and confiscation of assets

The vulnerability level associated with the effectiveness of confiscating criminal proceeds is medium.

The most recent amendment to the asset confiscation regulation, which was in force from 2020 to 2024, came into effect in 2017. A more modern and effective seizure and confiscation regulation, along with an increase in the number of competent officials in investigative bodies and various procedural stages, would reduce the exploitation of the Estonian financial system for money laundering and terrorist financing.

The legal framework for the seizure and confiscation of assets is fundamentally in place. Asset seizure is ensured by a court order upon the prosecutor's request (Code of Criminal Procedure § 142)⁵⁴. The FIU can, under the MLTFPA § 57, suspend a transaction or impose a restriction on the disposal of an account, the assets in the account, or other assets suspected of being involved in money laundering or terrorist financing for up to 30 calendar days, which can be extended if necessary.

It is possible to confiscate the means or direct object of the crime, the proceeds of the offense, and assets acquired with such proceeds. The institution of extended confiscation of criminal proceeds has been established (Penal Code § 83²). Upon the prosecutor's request and by the order of the preliminary investigation judge, it is possible to apply security measures to ensure state confiscation or substitute confiscation, such as asset seizure, judicial mortgage, and other measures permitted by the Code of Civil Procedure for securing a claim. During the observed period, Estonia also applied the seizure and confiscation of cryptocurrencies. It is possible to substitute the confiscation of assets subject to extended confiscation, i.e., if the assets cannot be taken, it is possible to recover an amount equivalent to the value of the assets subject to confiscation from the person (Penal Code § 84).

According to § 126 (2¹) of the Code of Criminal Procedure, assets seized to ensure confiscation can be sold upon the prosecutor's request and with the owner's consent, and by the order of the preliminary investigation judge. Assets can be sold without the owner's consent if the cost of holding them is unreasonably high or if it is necessary to prevent a significant decrease in the value of the assets.

⁵² In force since 01.01.2025.

⁵³ Cash declaration [Sularaha deklareerimine | Maksu- ja Tolliamet](#)

⁵⁴ In urgent cases, assets can be seized, with the preliminary investigation judge being notified within 24 hours, who then decides on the admissibility of the seizure within 72 hours.

As a vulnerability, attention should be drawn to the Supreme Court’s decision No. 3-23-2858⁵⁵ of March 31, 2025, where the Supreme Court explained the possibilities of state confiscation of assets suspected of money laundering and highlighted deficiencies in the current law. The Supreme Court emphasized that assets suspected of money laundering can only be confiscated in administrative proceedings if it is not possible to confiscate the assets during criminal proceedings for a valid reason. In its decision No. 3-24-1840 of June 12, 2025, the Supreme Court clarified its previous positions and confirmed the existence and use of administrative confiscation capabilities.

In 2024, a working group initiated by the Ministry of the Interior presented a report on the financial impact of crime with 69 proposals to reduce the incentives for financially motivated crime and significantly increase the identification, seizure, and confiscation of criminal proceeds⁵⁶. The implementation of the proposals involves significant roles for the MoJD, Mol, and MoF. The most important proposals concern the expansion of asset seizure and confiscation, the provision of confiscation without a conviction, the creation of a central asset management framework with a corresponding IT program solution, the establishment of a sustainable training system, and the adoption of IT solutions along with an increase in human resources.

Table 17. Value of assets seized in criminal cases sent to the prosecutor for further procedural decisions by year

Year	Value of assets seized in Estonia	Value of assets confiscated in Estonia
2020	10.8	2.2
2021	7	1.4
2022	18.4	2.4
2023	24.5	2.4
2024	68.2	4.1

Source: Ministry of Interior

From 2020 to 2022, investigative bodies and the prosecutor’s office seized assets worth an average of 12 million euros per year in criminal proceedings, and courts confiscated assets worth an average of 2 million euros per year through final court decisions. The search for reasons for the difference in the size of seizures and confiscations has so far found that during the court proceedings stage, the financial impact on crime is primarily achieved through measures to secure property claims, compensation for damages, and confiscations, in a total amount similar to the volume of seized assets. Extended confiscation of assets was applied in only one-third of the observed criminal proceedings⁵⁷.

In 2023–2024, the volume of asset seizures, including the amount of confiscated assets, increased, but the value of assets seized in criminal cases sent to the prosecutor increased mainly due to one large case per year, which does not indicate planned positive development but rather a random success. Additionally, it should be noted that the maintenance and storage costs of seized assets (primarily vehicles) can become unreasonably high due to the inability to dispose of the assets, which, upon the final court decision, reduces both the amount transferred to state revenues and the so-called fixed costs that the procedural body must bear to maintain the value of the assets.

⁵⁵ [3-23-2858/48](#)

⁵⁶ Report of the Working Group on the Financial Impact of Crime [Kuritegevuse varalise mõjutamise tööühma raport.pdf](#)

⁵⁷ Ombler, M. 2024. Short Analysis to Find Possible Reasons for the Differences in the Volumes of Seized and Confiscated Assets in Criminal Proceedings. Ministry of the Interior. https://www.siseministeerium.ee/sites/default/files/document-s/2025-01/L%C3%BChianal%C3%BC%C3%BCs%20varade%20arestimise%20ja%20konfiskeerimise%20vahe%20v%C3%B5imalike%20p%C3%B5hjuste%20leidmiseks_02.10.2024.pdf

3.2.3. Data sources

In summary, the overall rating given to data sources indicates a **higher than average level of vulnerability**, highlighting the need to improve data quality, systematized data collection, and the use of real-time accessible statistics in the fight against money laundering.

The main bottleneck in assessing money laundering risk in Estonia is insufficient and inconsistent statistics, which are not collected regularly based on common agreed principles. Data collection does not follow the objective⁵⁸ of gathering the necessary data for conducting a national risk assessment. The fragmentation and lack of timeliness of data complicate both operational decision-making and long-term strategic planning. The goal should be to achieve real-time accessible data collected based on a consistent and unified methodology, which would support government leaders and policymakers in making higher quality management decisions. This requires closer cooperation with all relevant parties and harmonizing the methods used to collect, validate, and analyze data. Such an approach would allow Estonian authorities to better understand threats and risks, allocate resources more effectively, and strengthen the anti-money laundering framework as a whole.

Possible mitigation measures could include automating the data collection necessary for the national risk assessment and creating a real-time risk visualization tool.

On the positive side, obligated entities have access to relevant and high-quality data sources to fulfill their obligations. Necessary guidelines can be found on the websites of the Financial Supervision Authority, the FIU, and the Ministry of Finance. There are also paid national databases that are actively used. On the negative side, smaller companies have more limited access to paid data sources, as the service is considered expensive.

a) Register of Beneficial Ownership

The vulnerability level for identifying beneficial owners is below average. The existence of a publicly accessible national register reduces the level of vulnerability. However, the vulnerability is increased by the data quality issues and lack of supervision of the register in use.

Since April 14, 2023, the Ministry of Finance has established the Beneficial Ownership Data Register (TEKSA)^{59,60}. The aim of TEKSA is to increase the transparency of companies, non-profit organizations, foundations, and trusts registered in Estonia by collecting, storing, and disclosing information. However, there are reliability issues with TEKSA data. The data is not kept up-to-date, which complicates the identification of beneficial owners. Identifying the beneficial owners of foreign legal entities is particularly challenging. This problem arises from the complexity and international dispersion of the legal entities' structures, which hinders the determination of ultimate beneficial owners. Ensuring the accuracy of the data is also complicated because the registrar does not have the ability to independently modify the data, making it solely the responsibility of the obligated entity to ensure the accuracy of the data. The state has the right to supervise the submitted data and initiate administrative proceedings and fine individuals in case of detected false data, but no such proceedings were conducted during the observed period. On the positive side, if, according to § 20 (2⁴) of

⁵⁸ See more details in section 3.2.4. b.

⁵⁹ Minister of Finance's Regulation No. 22 "Establishment and Statutes of the Beneficial Owners Data Register" adopted on 06.03.2023 and entered into force on 14.04.2023: It specifies the technical details of determining and registering beneficial owners, as well as their submission and publication in the Commercial Register, etc. This regulation established the Beneficial Owners Data Register (abbreviated as TEKSA) on 14.04.2023. The purpose of maintaining TEKSA is to increase the transparency of companies, non-profit organizations, foundations, and trusts registered in Estonia by collecting, storing, and disclosing information:

1. About the beneficial owners of private legal entities, except for those mentioned in § 76 (3) of the MLTFPA;
2. About trustees whose residence or registered office is in Estonia, and the trusts they manage;
3. About the entries mentioned in § 77-2 (3) of the MLTFPA.

⁶⁰ The Commercial Register does not allow the history of beneficial owners' data to be changed. [Äreregister ei võimalda tegelike kasusaajate andmete ajalugu muuta | Eesti | ERR](#)

the MLTFPA, an obligated entity becomes aware of information that differs⁶¹ from the data entered into the beneficial owners' data register while applying due diligence measures, the obligated entity must notify the registrar of the Business register of the discrepancy within a reasonable time. If the data is not corrected, the registrar can add a note to the data indicating doubts about its accuracy.

Identifying politically exposed persons (PEPs) is a significant challenge for everyone, as there is no central register in Estonia that includes such individuals. This makes identification complex and time-consuming, often requiring manual checks from multiple sources. As a result, the assessment of money laundering risks may be incomplete, as PEPs can have significant influence and connections to financial transactions. Creating a register of PEPs would significantly improve the effectiveness of risk assessment and reduce the risk of financial crimes.

b) Identity Verification

The vulnerability level associated with identity verification is below average. A positive factor is Estonia's strong technological identification system, while potential risks are considered to arise from the adoption of new technologies, such as artificial intelligence and deepfake technology.

The availability of a reliable identification infrastructure in Estonia is generally good due to the widespread use of ID cards, Mobile-ID, and Smart-ID, as well as the strong know-your-customer (KYC) and due diligence procedures of obligated entities (e.g., banks, payment service providers). However, there are vulnerabilities, the most significant of which are the limitations in background checks for foreign individuals and the risks of identity theft if remote identification processes do not fully comply with guidelines. The risks associated with Smart-ID stem from the fact that the use of Smart-ID is not linked to the validity of national documents.

Although Estonia has a strong national identity management system and high-level eID tools, additional measures are needed to ensure identity verification, prevent identity fraud and misuse, and avoid online scams.

3.2.4. Strategy, policy and ML crime definition

The overall assessment of the areas discussed in this chapter above **average vulnerability level**. Factors that increase vulnerability include the state's inability to systematically collect data for conducting national risk assessments and the decreased attention to combating money laundering at the national level.

a) National AML and CFT Strategy

A positive factor that reduces the level of national vulnerability is the regular preparation of a national risk assessment (NRA)⁶² in Estonia, one of the objectives of which is to provide clear recommendations to improve the quality of anti-money laundering measures. Analyzing the strategic documents of various state institutions (FSA, Prosecutor's Office, FIU, PBGB), it can be noted that financial crime has been given greater attention, as confirmed by Estonia's Internal Security Development Plan for 2020–2030⁶³. The FSA has prepared an AML strategy for 2022–2025⁶⁴, which focuses on a crucial area to ensure the stability and security of the financial system.

Regarding the FIU, it can be noted that strategic objectives are regularly reflected in their annual yearbook⁶⁵, providing an overview of the achievement of these objectives. A significant goal in the coming years is the

⁶¹ Submitting a Beneficial Owners Discrepancy Report [Tegelikelike kasusaajate lahknevusteate esitamine | Abiinfo](#)

⁶² National Risk Assessments, MoF. [Riskihinnangud | Rahandusministeerium](#)

⁶³ Internal Security Development Plan 2020-2030, MoI. [siseturvalisuse_arengukava_2020_2030_03.06.2021.pdf](#)

⁶⁴ AML Strategy 2022-2025, FSA. [fi_aml_jarelevalve_strateegia_2022-2025_1.pdf](#)

⁶⁵ FIU's Yearbooks. [Aastaraamatud | Rahapesu Andmebüroo](#)

development and implementation of the SAF. In March 2024, the Economic and Corruption Crimes District Prosecutor's Office⁶⁶ was established. This is an independent nationwide district that consolidates the competence and jurisdiction for handling significant economic crimes. A positive factor during the period under review is the existing legislation⁶⁷, which ensures that the organizational framework for policy formulation and implementation is regulated, transparent, and in compliance with international standards and EU law.

However, a factor that increases national vulnerability, as highlighted by the analysis, is the lack of a unified anti-money laundering strategy expressing political will at the national level. This absence can negatively impact resource assessment and the updating of legal norms. Although the legal framework is strong and diverse, it is crucial to ensure uniform priorities, resources, and metrics within the system of institutions involved in anti-money laundering to achieve effective results. The lack of a unified strategy causes inconsistency and lack of coordination between different institutions, which in turn reduces the effectiveness of anti-money laundering efforts. This can create gaps in supervision and make it difficult for market participants to adapt to global threats and related trends. Timely and proactive updating of legal norms is essential to maintain competitiveness in international markets and protect the country's financial stability. This includes not only adapting existing legal norms but also considering and implementing new technologies and methods in risk management.

b) The effectiveness of the state's data usage

So far, a data-driven approach to collecting statistics has not been systematically resolved to ensure the availability of machine-readable basic data, which is essential for identifying and effectively assessing national threats and vulnerabilities. The previously prepared national risk assessments (2015 and 2021) provided comprehensive knowledge of what data is needed for national risk assessment and how to use it to measure effectiveness, but this knowledge has not been sufficiently considered to ensure automated data collection and the development of information systems.

A significant problem is that data from international cooperation and criminal proceedings, and the data identified during these processes, are not purposefully collected or stored. This data would provide an overview of internal and external threats, the extent of criminal proceeds⁶⁸, and would allow for the planning and measurement of the state's procedural resource usage, including compliance with FATF standards and requirements.

c) The Government Commission for the Prevention of ML and TF

One factor that reduces national vulnerability is the establishment of the Government Commission for the Prevention of Money Laundering and Terrorist Financing in Estonia, as mandated by law (MLTFPA § 12). The Government Commission is the primary mechanism for cooperation and coordination in the fight against money laundering and terrorist financing at the national level. The tasks of the Government Commission include monitoring the implementation of the action plan, developing anti-money laundering and counter-terrorist financing policies, proposing legislative amendments, and cooperating at the national level in the fight against money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

⁶⁶ Large-scale economic crime, Prosecutor's annual reports. [Suure kahjuga majanduskuritegevus | Prokuratuuri aastaraamatud](#)

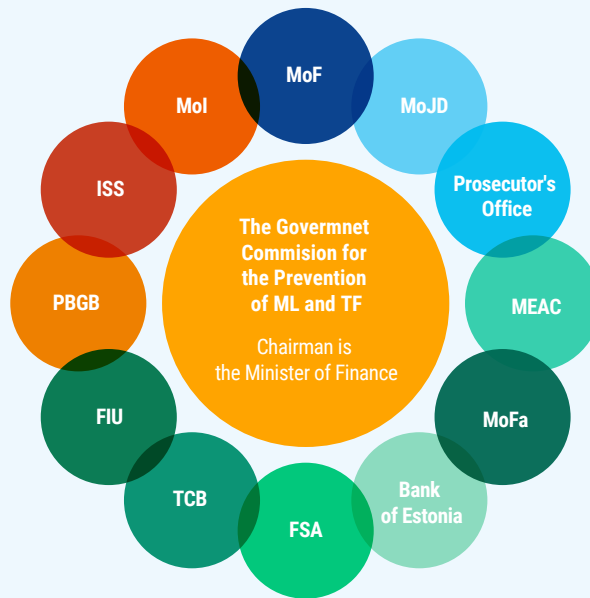
⁶⁷ The current MLTFPA establishes a clear obligation to prepare a national risk assessment.

⁶⁸ During the period under review, several analyses were conducted in Estonia regarding the extent of criminal proceeds. For example, M. Ombler's work "The Extent of Criminal Proceeds in Estonia. Analysis 2022" (<https://www.etis.ee/Portal/Publications/Display/f89ce7b1-ece5-40c7-a43d-2c885d2d88f0>) indicates that the extent of criminal proceeds from crime in Estonia could average 458 million euros per year.

According to another study, the volume of money laundering in Estonia could amount to approximately 1.49% of GDP, or about 637 million US dollars. For comparison, the total volume in the European Union is estimated at 438 billion dollars, and globally it reaches 3.1 trillion dollars (<https://verafin.com/wp-content/uploads/2025/03/European-Financial-Crime-Report-Nasdaq-Verafin-20250328.pdf>).

The Government Commission brings together all competent authorities and serves as the main mechanism for cooperation and coordination in the fight against money laundering and terrorist financing at the national level. The Government Commission is chaired by the Minister of Finance, and its members are listed in Figure 3.

Figure 3.
Composition of the Government Commission for the Prevention of Money Laundering and Terrorist Financing



Source: Ministry of Finance

The level of vulnerability is increased by the fact that the work of the Government Commission needs to be improved, as in recent years the active work and role of the Government Commission has remained more at the level of formal information exchange rather than substantive discussions and decisions, as illustrated by Table 18 below.

Table 18. Statistics on the agenda topics and substantive decisions of the Government Commission

Year	Number of Agenda Topics	Number of Substantive Decisions	Summary of Decisions
2020	24	3	Approval of the action plan for preparing for the MONEYVAL evaluation visit, including feedback collection.
2021	22	7	Approval of the NRA report and its subsequent action plan, along with confirmation of modifications to the MONEYVAL evaluation visit preparation plan.
2022	19	3	Collection of proposals for the sectoral strategy document draft and establishment of a subcommittee.
2023	9	4	Processing of decision drafts based on subcommittee proposals, feedback collection regarding U.S. advisory input and MONEYVAL evaluator candidates.
2024	2	1	Presentation of national risk assessment plans, including an introduction to the post-MONEYVAL action plan through written procedure (remained unapproved).
total	75	18	75% of decisions were categorized as "For Information Only," while only 25% were substantive.

Source: Ministry of Finance

The Government Commission lacks the authority to impose mandatory objectives on state institutions and allocate financial resources for the implementation of these objectives. According to the analysis, this hinders the creation of a unified national strategy and the fulfillment of the tasks set out in § 12 of the MLTFPA. In conclusion, it must be acknowledged that the Government Commission could be more effective in shaping the nationwide anti-money laundering and counter-terrorist financing policy.

d) Definition and Penalties for Money Laundering Crimes

Estonia has a strong regulatory framework for criminal penalties, supported by a separate criminal offense for money laundering agreements (PenalCode § 394¹), which is unique compared to other countries. However, enforcement activities face difficulties due to the high burden of proof and procedural complexity. Although the fines for administrative offenses related to money laundering violations have significantly increased during the assessment period, and the grounds for the criminal liability of legal entities have been expanded⁶⁹, the effectiveness of proceedings in the financial sector is still hindered by the time limits of administrative proceedings and the complexity of interviewing individuals residing abroad.

The composition of the money laundering crime and the responsibility for its commission are stipulated in the Penal Code. However, the Penal Code does not define the concept of money laundering, which is derived from the MLTFPA.

Estonia has adopted the European Union Directive (EU) 2018/1673 on combating money laundering by means of criminal law. Additionally, both the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198, Warsaw Convention) have been ratified. Both Article 3 of the aforementioned directive and Article 7 of UNTOC and Article 9 of the Warsaw Convention provide minimum standards for the composition of the money laundering crime and the necessary criminalization.

During the period under review, there have been instances in case law where courts have interpreted the law and the concept of money laundering more narrowly, thereby limiting the use of the possibilities provided by the law. According to the working group, the judges' interpretations of the money laundering norm are narrower than those allowed by international standards and conventions, which ultimately hinders the prosecution and judicial investigation of money laundering.

Handling complex cases, including identifying predicate offenses in connection with international cooperation, is time-consuming, and there is a risk that crimes may expire before or during court proceedings. Criminal cases have become significantly more extensive, cross-border, and procedurally complex due to the specialization of criminals and the use of information age tools. These factors, in turn, lead to insufficient time for conducting court proceedings for hidden crimes (especially economic crimes, including money laundering), as the time required for pre-trial proceedings is extended. Additionally, considering the length of court proceedings for extensive criminal cases, it is not justified that a case could expire in court proceedings due to the complexity of the proceedings. It should also be noted that, compared to the current regulation of the statute of limitations for offenses, a significant change has been the introduction of a reasonable time for proceedings into legal practice, which effectively keeps the proceedings in check and prevents unjustified delays.

The FIU has also identified statute of limitations issues during the conduct of administrative proceedings, which do not allow the state to be effective in anti-money laundering activities. The statute of limitations is also a problem when the competent authority identifies an act punishable by administrative proceedings within a reasonable time after its commission. The current legal order allows individuals to avoid the realization of

⁶⁹ https://www.juridica.ee/article_full.php?uri=2023_4-5_muudatused_juriidilise_isiku_s_teovastutuses&pdf=1

punitive objectives in certain cases. The FIU has identified various schemes that enable intentional delays in proceedings, leading to the expiration of the statute of limitations for administrative proceedings before a final decision is reached. The FIU has significantly enhanced its supervisory activities in recent years, resulting in an increase in identified violations. However, the limitation of administrative offenses and the descriptions of financial administrative offenses need to be reviewed to ensure they correspond to the issues identified during supervision.

3.2.5. The effectiveness of domestic and international cooperation

The level of vulnerability in national and international cooperation is overall lower than average, as the state has established the necessary cooperation networks and the legal framework supports cooperation in the field of anti-money laundering.

a) Effectiveness of National-Level Cooperation

Estonia has established a solid legal framework for combating money laundering and terrorist financing, which enables effective cooperation between supervisory, investigative, and law enforcement agencies. At the operational level, an expert working group led by the FIU has been established, including the FSA, the PBGB, the ISS, the Prosecutor's Office, the TCB, and the Foreign Intelligence Service. Regular meetings (at least quarterly) have significantly improved information exchange, case resolution, and typology identification, thus operational cooperation is highly valued.

Cooperation with obligated entities is generally positive, and during the period under review, cooperation between the public and private sectors was enhanced. The Government Commission for the Prevention of Money Laundering and Terrorist Financing plays a role in promoting cooperation, ensuring nationally coordinated action in both strategic policy and risk mitigation plans.

Significant progress has been made in public-private partnership projects, such as the Estonian Financial Intelligence Working Group (EFIT) launched in 2024, which brings together the FIU and major banks to share case-specific and strategic information more efficiently. Additionally, the FIU has joined Europol's European Financial Intelligence Public-Private Partnership (EFIPPP), providing a common platform for cross-border information exchange. This strengthens the risk-based approach, enabling quicker responses to new threat patterns at both national and international levels. Cooperation between investigative agencies (PBGB, ISS, Prosecutor's Office, TCB) and the FIU, for example in imposing asset restrictions or in strategic/tactical analysis, has become significantly more effective in recent years, as evidenced by the increase in the value of seized/confiscated assets during the period under review.

The FSA effectively cooperates with both the public and private sectors. Anti-money laundering cooperation meetings and training activities are ongoing. For example, the FSA regularly participates in the Banking Association's anti-money laundering and sanctions working group meetings. Additionally, since January 2022, the Financial Supervision Authority has been a member of the national implementation steering group for international sanctions. The effectiveness of national-level cooperation is also demonstrated by the regular public-private cooperation project organized by the FSA – the Anti-Money Laundering and Counter-Terrorist Financing Information Day, which has seen high participation⁷⁰ participation among supervisory subjects.

In conclusion, operational-level cooperation in Estonia is very good, and cooperation mechanisms are in place.

⁷⁰ 1) On 27.06.2024, 356 people participated; 2) On 08.06.2023, 385 people participated; 3) On 16.11.2023, 327 people participated. These participant numbers do not only reflect credit and financial institutions under the supervision of the FSA, but also other financial institutions, non-financial service providers, interest groups, and their representatives.

However, the national-level coordination structure (Government Commission) needs clearer leadership and a more effective decision-making process to elevate national-level cooperation as a whole. A vulnerability that can be highlighted is the limited involvement of the Environmental Board in anti-money laundering cooperation groups.

b) Effectiveness of International Cooperation

Estonia ensures mutual legal assistance based on international treaties, conventions, generally recognized principles of international law, and the regulations on international cooperation in the Code of Criminal Procedure (Chapter 19). Estonia has established an adequate legal framework for effective international cooperation. The analysis conducted for this report concluded that while Estonia has a sufficient legal framework for effective international cooperation, there is still a need to update the entire part of the Code of Criminal Procedure related to criminal proceedings and to systematically rethink its general part and various instruments.

Effective international cooperation is primarily possible through legal assistance requests and European Investigation Orders, and Estonia utilizes these opportunities. The current law also allows for the creation of joint investigation teams⁷¹ and participation in their activities. Participation in the activities of investigation teams enables prosecutors to quickly exchange data and evidence in cross-border crime proceedings without additional procedures. Additionally, three delegated prosecutors have been appointed in Estonia to handle crimes committed in Estonia that fall under the jurisdiction of the European Public Prosecutor's Office (EPPO) and affect the EU's financial interests.

Table 19. Statistics on mutual legal assistance requests (MLA)⁷² and european investigation orders (EIO)⁷³ related to money laundering received in Estonia from 2020 to 2024

	2020		2021		2022		2023		2024	
	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO
Received	36	133	31	121	20	121	21	121	19	101
Completed	36	128	27	117	19	119	20	115	18	99
Rejected, including cases where fulfillment was impossible	0	5	4	4	1	0	1	4	1	2
Average Processing Time (in Days)	130	79	96	62	95	59	81	48	70	51

Source: Prosecutor's Office

Table 20. Statistics on mutual legal assistance requests (MLA) and european investigation orders (EIO) related to money laundering sent from Estonia from 2020 to 2024

	2020		2021		2022		2023		2024	
	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO
Received	20	56	25	45	14	23	16	30	19	25
Completed	17	49	20	41	6	3	10	24	7	12
Rejected, including cases where fulfillment was impossible										
Average Processing Time (in Days)	208	119	143	92	201	119	155	65	131	52

Source: Prosecutor's Office

⁷¹ Joint investigation team.

⁷² Legal assistance request.

⁷³ European Investigation Order.

The statistics on European Investigation Orders and legal assistance requests (see Tables 19 and 20) show that more European Investigation Orders are submitted and sent in international cooperation than legal assistance requests. Refusals of international cooperation are rare and only occur in justified cases. These are primarily requests from foreign countries that have been impossible to fulfill (for example, the request contains deficiencies and the requested country does not respond to additional questions; the requested country has used the wrong instrument; the person for whom the procedural action was requested is not in Estonia; it is a legal assistance request from Russia or Belarus). On average, Estonia takes significantly less time to fulfill requests than foreign countries.

Table 21. Requests for seizure received in Estonia from 2020 to 2024

	2020			2021			2022			2023			2024		
	ML	TF	Other	ML	TF	Other	ML	TF	Other	ML	TF	Other	ML	TF	Other
Received	2	0	13	2	0	21	5	0	17	7	0	17	5	0	20
Completed	0	0	4	0	0	9	3	0	6	5	0	7	2	0	6
Rejected	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Impossible to complete	2	0	9	2	0	12	2	0	11	2	0	10	2	0	12

Source: Prosecutor's Office

Table 22. Requests for asset seizure sent from Estonia from 2020 to 2024

	2020			2021			2022			2023			2024		
	ML	TF	Other	ML	TF	Other	ML	TF	Other	ML	TF	Other	ML	TF	Other
Received	0	0	7	13	0	5	1	0	5	0	0	6	0	0	0
Completed	0	0	4	n/a	0	n/a	n/a	0	n/a	0	0	2	0	0	0
Rejected	0	0	3	n/a	0	n/a	n/a	0	n/a	0	0	n/a	0	0	0

Source: Prosecutor's Office

The statistics on seizure requests (Tables 21 and 22) show that from 2020 to 2024, the number of seizure requests sent from Estonia is smaller than the number of seizure requests received in Estonia. Over five years, Estonia has submitted only 37 seizure requests, 14 of which are related to money laundering suspicions. Notably, in 2023 and 2024, Estonia did not submit any seizure requests related to money laundering, even though Estonia is a transit country for funds suspected of money laundering. Additionally, the practice of submitting requests varies between countries. Estonia sends a seizure request only when it is known that the asset exists in a foreign country. In contrast, seizure requests received from foreign countries in Estonia mostly remain unfulfilled because the asset is not actually in Estonia.

Table 23. Confiscation requests received in Estonia from 2020 to 2024

	2020			2021			2022			2023			2024		
	ML	TF	Other	ML	TF	Other	ML	TF	Other	ML	TF	Other	ML	TF	Other
Received	0	0	8	0	0	6	0	0	6	0	0	4	0	0	7
Completed	0	0	5	0	0	5	0	0	3	0	0	2	0	0	5
Rejected	0	0	0	0	0	3	0	0	0	0	0	0	0	0	
Impossible to complete	0	0	3	0	0	0	0	0	3	0	0	2	0	0	2

Source: Prosecutor's Office

From 2020 to 2024, Estonia did not receive any confiscation requests related to money laundering (Table 23). The small number of seizure and confiscation requests indicates that the effectiveness of international cooperation in seizing crime instruments and criminal proceeds is low.

To share information, competent authorities for international criminal procedure cooperation use international law enforcement networks such as the Egmont Group, Europol, Eurojust, Interpol, EPAC/EACN, CARIN, PWGT, and others. Additionally, the PBGB, the ISS, and the TCB have secure communication channels for international cooperation (e.g., SIENA) and liaison officers and sectoral networks. For example, representatives from PBGB and TCB are permanently seconded to Europol's liaison officers' office, and Finland's customs liaison officer representing the Nordic countries, as well as liaison officers from Germany, the UK, and the USA for the Baltic States, are based in Estonia, facilitating the exchange of information needed for both criminal and administrative proceedings. Supervisory authorities have appropriate cooperation channels for daily international cooperation and information exchange.

The FIU has effective international cooperation – the FIU assists Estonian investigative authorities in international cooperation and helps use the information obtained during international cooperation in analysis and sharing within Estonia. The FIU effectively uses foreign information in initiating and conducting its case analyses, including making foreign inquiries, the analysis results of which are forwarded to investigative authorities.

The FSA conducts international cooperation in the field of anti-money laundering with other countries (Sweden, Finland, Latvia, Lithuania, Denmark, and Germany, as well as several third countries) based on mutual cooperation agreements. Most international cooperation takes place under EU directives and does not require the conclusion of mutual cooperation agreements. The FSA is represented in several anti-money laundering colleges, aimed at ensuring effective international cooperation and information exchange between competent financial supervisory authorities. The FSA has established and leads five colleges and participates in the work of 14 colleges initiated by other supervisory authorities. At the Baltic level, the Baltic Sanctions Task Force has been operating since October 2022, involving both the FSA and FIU. Additionally, the Financial Supervision Authority participates in the Nordic-Baltic Working Group established to strengthen cross-border anti-money laundering cooperation at the Nordic and Baltic levels. Within the framework of international cooperation, information is shared through information exchange platforms created by the European Banking Authority (EuReCA and E-Gate databases).

4. ML Vulnerabilities of the Financial Sector

4.1. Description of the Methodology

The sector's vulnerability to money laundering is low if its capacity to prevent money laundering is high. The higher the level of sector vulnerability, the weaker or less effective the anti-money laundering activities in that sector are.

To assess the various fields of the financial sector (sub-sectors and products), the World Bank offers several assessment modules, which are largely similar in structure and based on the evaluation of the following criteria or factors:

- The extent of the anti-money laundering legal framework
- The effectiveness of supervisory procedures and practices
- The existence and enforcement of administrative penalties
- The existence and enforcement of criminal penalties
- The existence and effectiveness of entry controls
- The commitment of company employees
- The awareness of company employees regarding money laundering risks
- The effectiveness of the compliance function
- The effectiveness of monitoring and reporting suspicious transactions
- Market pressure to comply with anti-money laundering standards
- The availability and access to information about the beneficial owner
- The availability of a reliable identification infrastructure
- The availability of independent information sources

The last three criteria were also assessed in the national vulnerability module, which is why these topics were covered more thoroughly in the national vulnerability chapter.

The module distinguishes between two types of variables: input and intermediate variables. Input variables are further divided into anti-money laundering control variables, which apply to the entire sector, and inherent vulnerability variables, which are related to the specific characteristics of the sector. Intermediate variables represent combinations of multiple input variables and are assessed indirectly through input variables. The impact on vulnerability can be direct or indirect, and the importance of one factor often depends on the presence of others. In assessing inherent vulnerability, the sector's specifics and need-based indicators are considered, such as the profile of the product or service's customer base, the level of cash transactions associated with the product, the frequency of international transactions, the use of agents in offering the product, non-face-to-face interaction with customers, and the anonymity of the service.

The World Bank's methodology divides the financial sector into four major areas: banking, investment, insurance, and other financial services. Tools have been created for assessing each area at both the sector

and specific product levels. The working group used various modules to assess different market participants and their products (see Table 24).

Table 24. Modules used in the assessment of sub-sectors and products in the financial sector.

Market participants in the financial sector	Vulnerability assessment module
Credit Institutions	Module 3 Banking Sector Vulnerability
Branches of Foreign Credit Institutions in Estonia	
Investment Firms	Module 4.A Securities Sector Vulnerability
Branches of Foreign Investment Firms in Estonia	
Licensed Fund Managers	Module 4.A Securities Sector Vulnerability
Licensed Small Fund Managers	
Registered Small Fund Managers	
Voluntary Pension Funds	Module 4.B Securities Sector Vulnerability - Product Based
Life Insurers	Module 5 Insurance Sector Vulnerability
Branches of Foreign Life Insurers	
Insurance Brokers	
Payment Institutions	Module 6.B Other Financial Institutions Vulnerability - Product Based
Branches of Foreign Payment Institutions	
E-Money Institutions	
Payment Agents of Estonian Payment Institutions operating in Estonia	
Payment Agents of Estonian Payment Institutions Operating Abroad	
Currency Exchange Service Providers	Module 6.A Other Financial Institutions Vulnerability
Savings and Loan Associations	Module 6.A Other Financial Institutions Vulnerability
Credit Providers	Module 6.B Other Financial Institutions Vulnerability - Product Based
Credit Intermediaries	
Loan Providers	
Leasing Providers	
Providers of collateral and guarantee transactions	

In the assessments based on the listed criteria, both qualitative and quantitative data were used: the experience and expert opinions of the working group's experts, statistics from supervisory and law enforcement agencies' proceedings, court decisions on money laundering cases, data from the Financial Supervision Authority's analytical tool, the experience and feedback of market participants (focus group interviews, written surveys, discussions at working group meetings).

4.2. General Developments and Vulnerabilities of the Financial Sector

The Estonian financial sector is of medium size in international comparison.⁷⁴ As of the fourth quarter of 2024, the resources⁷⁵ utilized by the financial sector amounted to 189% of Estonia's GDP for the four quarters of 2024.⁷⁶

A Brief Overview of the Most Significant Money Laundering Threats⁷⁷ in the Financial Sector:

- The level of cross-border money laundering risk remains highest in payment services of credit institutions, especially in **connection with correspondent services for foreign fintech companies**.
- Suspicious funds continue to be moved through virtual accounts, also known as **VIBANs**.
- Credit institutions have also been involved in cases of sanctions evasion.
- Although the number of reports related to **correspondent accounts** has decreased, this rather indicates the termination of business relationships with individual partners, not the disappearance of the risk.
- Cross-border payment and e-money services are increasingly used to conceal criminal activities in cash transactions.
- While cash usage among the Estonian population is decreasing, the number of cash-related money laundering reports and foreign inquiries has significantly increased. This indicates a continuing risk, especially in the areas of traditional cash transfer services and currency exchange.

The Estonian financial sector is bank-centric, which means that the credit institution sector has a significant impact on the entire financial sector's vulnerability to money laundering.

Table 25. Market shares of financial sector participants by sector as of 31.12.2024

Sector	Payments	Investment products and funds	Loans	Deposits
Credit Institutions	99.8%	70.5%	95.2%	99.7%
Fund Managers		25.1%		
Investment Firms		4.4%		
Payment Institutions	0.2%			
Credit Providers ⁷⁸			4.5%	
Savings and Loan Associations			0.3%	0.3%

Source: FSA, Bank of Estonia

Under the MLTFPA, obligated entities include both credit and financial institutions, which are supervised by either the FSA or the FIU according to their respective licenses. The list of obligated entities in the financial sector covered in this risk assessment is provided in the table below. Market participants need more clarity on the definitions and boundaries of various financial services, as well as the division of supervisory

⁷⁴ Bank of Estonia, Overview of the Structure of the Financial Sector, p. 4. https://haldus.eestipank.ee/sites/default/files/2023-07/fsr2023_est.pdf

⁷⁵ The resources of the financial sector include deposits raised, loan obligations, issued debt securities, the net value of units of pension and public investment funds, and the technical reserves of insurers.

⁷⁶ Bank of Estonia, Financial Accounts Statistics for the fourth quarter of 2024. <https://www.eestipank.ee/press/statistikateade-maksumuudatuste-ootus-suurendas-aasta-lopus-majapidamiste-finantsseisu-14042025>

⁷⁷ See for more details Chapter 2.

⁷⁸ Credit providers, credit intermediaries, lenders, lessors, and providers of collateral and guarantee transaction services.

responsibilities between the FSA and the FIU⁷⁹, particularly concerning small fund managers, savings and loan associations, and loan services.

During the preparation of this risk assessment, no evaluation was made of the vulnerability of money laundering risks for crowdfunding service providers, as during the assessment period, crowdfunding service providers were not considered obligated entities under the MLTFPA. Although the previous risk assessment highlighted several forward-looking threats related to the rapid growth of crowdfunding service providers, these threats have not significantly impacted the financial sector. By the end of the assessment period, there were only two market participants with a license for crowdfunding services. Other participants in the loan and investment market offering services based on the crowdfunding model were assessed according to the licenses issued to them in the loan and investment services modules.

Table 26. Sectors assessed in the financial field

Financial sector participants	Supervisory authority	Number of participants as of 31.12.2024	Threat	Vulnerability
Credit Institutions	FSA	9	Above average	Medium
Branches of Foreign Credit Institutions in Estonia	FSA	5		
Investment Firms	FSA	8	Medium	Medium
Branches of Foreign Investment Firms in Estonia	FSA	1		
Licensed Fund Managers	FSA	12	Medium	Above average
Licensed Small Fund Managers	FSA	6		
Registered Small Fund Managers	FIU	81 (70) ⁸⁰		
Voluntary Pension Funds	FSA	17		Below average
Life Insurers	FSA	2	Low	Low
Branches of Foreign Life Insurers	FSA	3		
Insurance Brokers⁸¹	FSA	12		
Payment Institutions⁸²	FSA	16	Above average	Medium
Branches of Foreign Payment Institutions	FSA	2		
E-Money Institutions	FSA	3		
Payment Agents of Estonian Payment Institutions operating in Estonia	FSA	2		
Payment Agents of Estonian Payment Institutions Operating Abroad	FSA	4		

⁷⁹ See also FIU Yearbook 2023, p. 45, https://fiu.ee/sites/default/files/documents/2024-04/Rahapesu%20Andmeb%C3%BCroo%20aastaraamat%202023_0.pdf

⁸⁰ Some small fund managers registered in the FSA's market participants register have not applied for a financial institution license from the FIU (the number of small fund managers with a FIU's license is indicated in parentheses).

⁸¹ The assessment took into account the activities of insurance brokers who mediated life insurance services during the assessment period, based on the exception stipulated in § 6 (2) point 5 of the MLTFPA.

⁸² Payment institutions that only offer account information and/or payment initiation services were excluded from the assessment, based on the exception stipulated in § 6 (2) point 2 of the MLTFPA.

Financial sector participants	Supervisory authority	Number of participants as of 31.12.2024	Threat	Vulnerability
Currency Exchange Service Providers	FIU	23	Medium	Below average
Savings and Loan Associations	FIU	14 ⁸³	Medium	Medium
Credit Providers	FSA	42	Medium	Medium
Credit Intermediaries	FSA	7		
Loan Providers	FIU	73		
Leasing Providers	FIU	25		
Providers of collateral and guarantee transactions ⁸⁴	FIU	7		

During the assessment period, the risk management capabilities of credit institutions and financial institutions have improved due to investments in risk control systems and employees, including through training. The risk awareness of market participants has also increased thanks to training and information, including typology reports, provided by state authorities on money laundering risks.

Recent global trends indicate the need to consider the rapid development of technology. Balancing the opportunities and risk controls arising from innovation helps ensure a safe and stable financial environment, and insufficient consideration of this makes financial sector participants vulnerable to various risks, including money laundering risks. During the assessment period, financial sector participants significantly invested in the development of automated monitoring and screening solutions, which have generally been brought to a good level. However, the effectiveness of automated solutions in the financial sector is not consistently at the same level across specific entities.

CASE STUDY⁸⁵

At the end of 2024, the FSA conducted a large-scale test to assess the capability of automated systems in a sample of credit and financial institutions to identify individuals and companies listed in sanctions lists. The test was carried out in collaboration with an external technology service provider. The use of modern technology in supervision allowed for extensive and large-scale testing of screening systems.

The test results showed that using good technology alone is not always sufficient. Effectiveness is higher when there are experts who understand the field of financial sanctions and can correctly configure the screening systems, adapting them to the needs or business model of the institution.

The sanctions lists used included international sanctions and those imposed by the Government of the Republic of Estonia, as well as lists from the UN, the European Union, and the United States. The test assessed the capability to find exact matches as well as variously manipulated names.

⁸³ By the end of 2024, there were 14 savings and loan associations in operation, two of which had been issued a payment institution license by the FSA. Consequently, the money laundering vulnerability of these two was assessed in the payment institutions module, while the sector's activity statistics are presented for all savings and loan associations.

⁸⁴ According to the Register of Economic Activities, as of 31.12.2024, there were a total of 80 financial institutions engaged in loan, leasing, collateral, or guarantee transactions under the supervision of the FIU. These are presented in the table below by sub-services, with some companies overlapping.

⁸⁵ <https://www.fi.ee/et/uudised/finantsinspektsioon-testis-finantsasutuste-sanktsioonide-kohaldamise-susteeme>

In assessing the vulnerability of the financial sector, the evaluations were consistently influenced by issues related to administrative and criminal penalties, which are described in more detail in the chapter on national vulnerabilities. Problems related to the availability and reliability of beneficial ownership information significantly affect the vulnerability of the entire financial sector. These issues are also addressed in more detail in the chapters on national vulnerabilities and legal entities.

The vulnerability of financial institutions operating under a FIU's license is affected by certain weaknesses in the legal framework concerning financial activity licenses, which are discussed in more detail below under various financial services. The main issues include the limited ability of supervision to effectively deal with market participants who have essentially ceased offering services or fail to provide necessary data, as well as license applications submitted by individuals not connected to Estonia. The challenge lies in effectively intervening in the provision of financial services without a license or under an incorrect license.

The FSA's activities in conducting entry controls and suitability assessments, as well as ongoing supervision, have been effective. The FSA has carried out risk-based supervision of credit and financial institutions, conducting numerous on-site and remote inspections and applying various enforcement measures, ranging from meetings with management to imposing fines as a result of misdemeanor proceedings. The capabilities of supervisory authorities are also described in section 3.2.1, point f for FIU and point g for the FSA.

Table 27. Number of inspections conducted by the FSA by sector

Market participants with a license from the FSA	Type of inspection	2020	2021	2022	2023	2024
Credit institutions and branches of foreign credit institutions	On-site inspections	2	8	1	1	14
	Remote inspections	63	28	29	14	27
Investments firms	On-site inspections	0	2	0	1	2
	Remote inspections	5	7	9	9	9
Fund managers	On-site inspections	0	0	0	1	0
	Remote inspections	0	16	5	19	0
Life insurers	On-site inspections	5	0	0	0	0
	Remote inspections	5	5	6	7	5
Payment institutions and e-money institutions	On-site inspections	3	0	0	0	4
	Remote inspections	24	31	39	21	19
Credit providers and intermediaries	On-site inspections	0	6	0	6	1
	Remote inspections	0	66	0	74	8

Source: FSA

During the period under review, the FIU conducted a total of 171 company-specific remote inspections and 7 on-site inspections in the financial institutions sector. Following the principle of a risk-based approach, FIU's supervisory unit focused primarily on mitigating the significant risks in the virtual currency service providers sector from 2021 to 2023. No on-site inspections were conducted in financial institutions during this period, which affected the sector's awareness and vulnerability. FIU's supervisory effectiveness increased in the latter half of the period under review (2023–2024) due to process improvements, additional resources, and capabilities.

In the spring of 2024, FIU's supervisory unit conducted a one-time mapping via an online survey among all companies with a financial institution license (approximately 290 companies at the time). This included remote

inspections of a total of 155 financial institutions (loan market participants and fund managers). Based on the remote inspection data, FIU identified the risk levels of specific market participants by service – by the end of the assessment period, risk matrices for lessors and fund managers were completed, and the risk matrix for lenders was being prepared – and continued to organize the financial institutions market and conduct risk-based on-site inspections.

Risk-based supervision is somewhat hindered by the fact that data on the activities of some financial sector participants, who are not covered by financial supervision, is not collected regularly. Since 2021, the MLTFPA includes an authorization norm (§ 54¹), which allows the minister responsible for the field to establish data submission procedures for all obligated entities. Among the financial institutions under the supervision of the FIU, only registered small fund managers and savings and loan associations have a regular data submission obligation. They submit statistical reports to the FSA and the Bank of Estonia, but unfortunately, these reports are not fully accessible to FIU as the supervisory authority for these sectors in the field of money laundering prevention, due to the restriction set out in § 454 (10) of the Financial Supervision Act (FIS)⁸⁶.

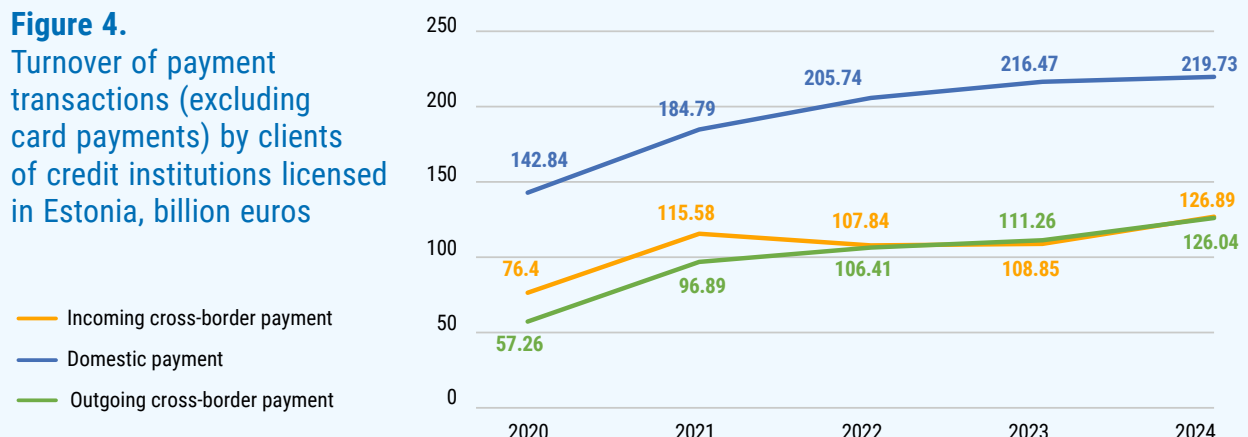
4.3. Credit Institutions

The level of money laundering vulnerability for credit institutions is **medium**.

The Estonian financial sector is bank-centric: the credit institution sector has a significant dominance in the provision of financial services. The market share of credit institutions is over 99% for payments, 71% for investment services, and 95% for loans (see Table 25). During the assessment period, there were 9 credit institutions and 5 branches of credit institutions registered in the European Union operating in Estonia. The sector has been relatively stable over the years, with the market share of smaller local credit institutions increasing.

The turnover of payments⁸⁷ by credit institutions grew from 276.5 billion euros in 2020 to 472.7 billion euros in 2024. The connection between the turnover of cross-border payments and the economy is indicated by the countries with the highest volumes of transactions for households and companies, which are Latvia, Lithuania, Finland, Germany, and Sweden. The share of cash payments⁸⁸ accounted for less than one percent of all payments, remaining steadily around 20 million euros each year.

Figure 4.
Turnover of payment transactions (excluding card payments) by clients of credit institutions licensed in Estonia, billion euros

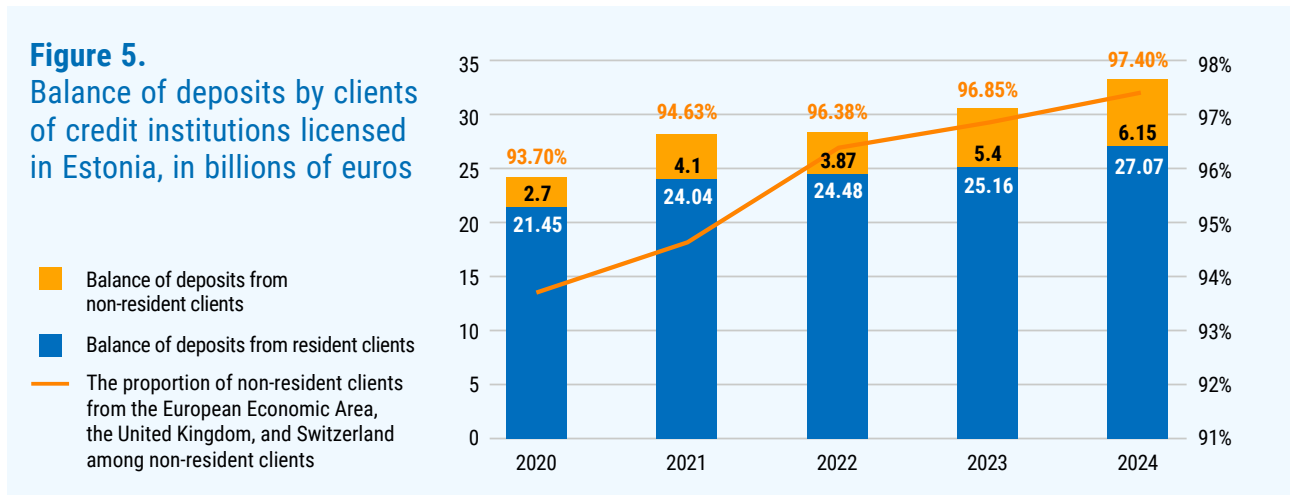


⁸⁶ Financial Supervision Authority Act.

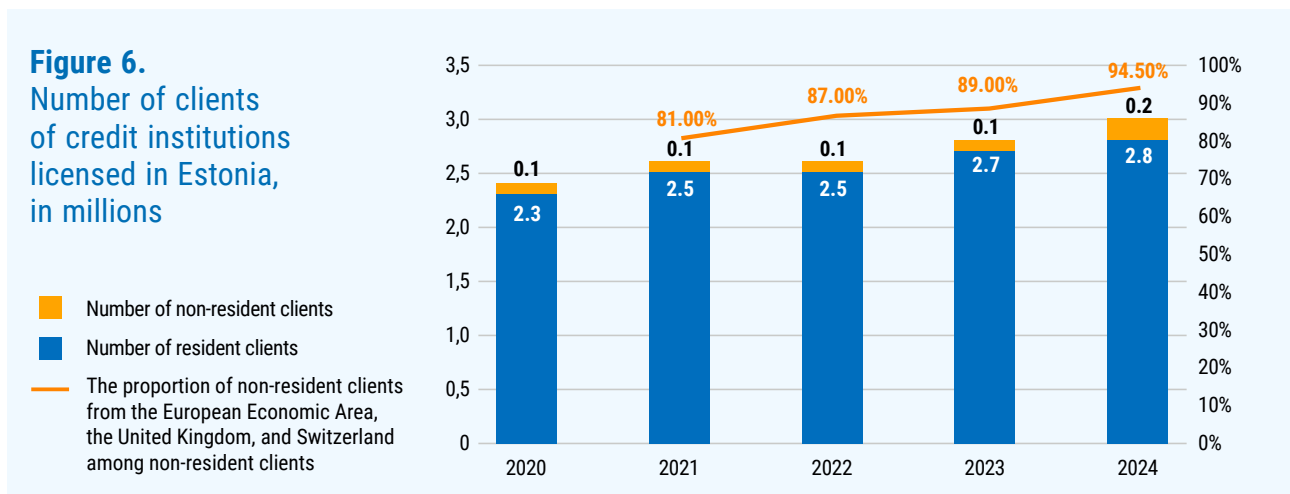
⁸⁷ Without card transactions.

⁸⁸ Without card transactions.

Similarly to the stable growth of payments, the deposits of credit institutions have also increased during the assessment period, reaching from 24.15 billion euros in 2020 to 33.22 billion euros in 2024.



As of 31.12.2024, credit institutions had 2.97 million clients, of which 95% were residents and 5% were non-residents. During the previous National Risk Assessment (NRA) period, higher risks were associated with the activities of non-residents, which led credit institutions to further analyze their client bases. As a result, the proportion of clients from higher-risk countries has decreased, meaning the risk profile of non-resident clients has become lower compared to the previous NRA period. Individual clients made up 89%, and legal entity clients made up 11%. The share of non-resident deposits has grown to levels comparable to those in 2015, but the structure of the deposits is significantly different. The volume of non-resident deposits is created by individuals who are residents of the European Union, primarily due to individuals from the Netherlands and Germany brought in through deposit platforms. The volume of deposits from clients in so-called offshore areas has decreased to nearly zero.



The number of clients from respondent institutions⁸⁹ at credit institutions has decreased annually during the assessment period: while at the end of 2021, credit institutions had 420 clients from respondent institutions, by the end of 2024, there were 306. Conversely, the total turnover of cross-border payments by clients from respondent institutions at credit institutions has increased annually during the assessment period: from 105.28 billion euros in 2021 to nearly 136 billion euros in 2024. The growth in the total turnover of cross-border payments is primarily driven by credit institutions' payment mediation to payment institutions and e-money institutions, with the total turnover of cross-border payments mediated to them being nearly 84 billion euros in 2024 (52.5 billion euros in 2021). Approximately 89% of the total turnover of cross-border payments consists of payment mediation to non-resident respondent institutions, which are primarily residents of the European Economic Area or the United Kingdom.

Table 28. Total turnover of cross-border payments mediated by credit institutions to respondent institutions in billions of euros

Respondent institutions	2021	2022	2023	2024
Clients from credit institutions	7.93	5.11	17.62	12.56
Clients from payment institutions and e-money institutions	52.53	71.68	72.30	83.99
Clients from investment firms	0.22	1.66	2.51	5.65
Clients from crowdfunding service providers	1.47	0.55	0.35	0.26
Clients from virtual currency service providers	43.12	33.02	21.06	33.54
Total	105.28	112.03	113.83	135.99
Other clients from financial institutions	N/A	N/A	N/A	1.56
Including other clients from financial institutions	N/A	N/A	N/A	137.55

Source: FSA

The vulnerability of the credit institution sector to money laundering at all stages (placement, layering, and integration) lies not only in the large volumes of services and the total number of clients but also in the speed of establishing business relationships and conducting transactions, as well as in the provision of correspondent services.

Although the provision of payment services in Estonia and globally has become increasingly fragmented, with various alternative payment channels and business forms emerging alongside conventional banking (such as transactions with crypto-assets, payment institutions, and e-money institutions), criminals still need banking services to conceal illegal assets. The provision of **correspondent banking** services carries an inherently higher level of risk. The vulnerability of credit institutions receiving payments is increased by the use of virtual IBAN accounts, or so-called VIBAN accounts. This is because the accounts opened at the credit institution are not used directly by clients in a business relationship with the credit institution, but by the clients of those clients. This means that the correspondent service provider has reduced knowledge of the ultimate beneficiaries of the transactions and the movement and purposes of the funds, depending on the control systems and risk awareness of the respondent institutions. VIBANs are used to mark sub-accounts associated with a single account (IBAN), often for providing correspondent services to other financial intermediaries and moving their clients' funds. The monitoring solutions used by institutions receiving payments are not

⁸⁹ A respondent institution is a financial institution that has a correspondent account relationship with another financial institution to carry out payments, settlements, or other financial services in regions or currencies where it does not have direct access. In this context, the data of clients from credit institutions, payment institutions and e-money institutions, investment firms, crowdfunding service providers, and virtual currency service providers were included in the consideration of respondent institutions.

capable of distinguishing whether a payment is received from a VIBAN account or a regular IBAN account. Therefore, VIBAN accounts obscure the actual location of the IBAN account (e.g., in a jurisdiction with a higher risk of money laundering) and the actual beneficiary. In cases where there is no public information about the use of a VIBAN account, the biggest challenges lie in the application of automated tools and the performance of manual checks.

The legal framework for credit institutions is comprehensive and multifaceted. The regulations and requirements are designed to broadly consider the various stakeholders in the sector and provide clear guidelines and requirements for market participants. This means that the provisions are generally precisely and clearly defined, which supports their implementation and compliance. Clear and specifically defined legal norms help market participants understand their obligations and responsibilities, ensuring consistent compliance with regulatory requirements. Clarity in the legal framework reduces interpretation problems and helps avoid potential violations, promoting the stability and reliability of the financial sector.

The FSA has ensured effective entry controls and suitability procedures in the banking sector. Ongoing supervision is carried out both cyclically and on a risk-based basis, with more attention directed to higher-risk market participants. During the assessment period, the FSA has updated the guidance⁹⁰ for market participants, adopted several guidelines from the European Banking Authority (EBA), and clarified the roles and responsibilities of credit institutions in providing primary payment services.⁹¹

As a positive trend, investments in managing money laundering risks in the banking sector have been steadily increasing. In 2024, a total of 100.2 million euros was invested in the anti-money laundering sector, nearly three times more than in 2021. The most significant increases have been in investments in technology (transaction monitoring and screening systems and customer management software) and personnel (salary costs). The number and quality of training sessions and the awareness of market participants have also increased. As a rising trend, banks are using testing for trainees and training based on exposure to risk factors and the nature of job tasks. Credit institutions have continuously improved their internal compliance frameworks and organizational solutions over time, including significantly enhancing internal controls (including quality controls). Credit institutions generally have clearly defined responsible persons for different lines of defense and thematic areas, such as anti-money laundering, sanctions compliance, and compliance control. Board members and responsible employees in the anti-money laundering field (including contact persons for the FIU) are generally subject to suitability procedures or similar compliance processes, which also mitigate the risk of internal fraud.

The sector has seen significant improvements in public-private cooperation, which is further detailed in the chapter on national-level cooperation (3.2.5.).

The compliance control function of credit institutions is generally well-developed, but supervision has identified underestimation of money laundering risks and overestimation of compensation mechanisms (resources), as well as deficiencies in identifying and analyzing suspicious situations and transactions, which have, among other things, stemmed from inadequate solutions for knowing customers.

Transaction monitoring is carried out daily in real-time and/or retrospectively, with additional ad hoc monitoring measures applied as necessary. Despite this, the screening and monitoring solutions used do not always match the risks taken by credit institutions.

⁹⁰ The FSA's recommended guidelines "Organizational Solution and Preventive Measures for Credit and Financial Institutions to Prevent Money Laundering and Terrorist Financing": https://www.fi.ee/sites/default/files/2024-06/Finantsinspektsiooni%20rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20juhend_0.pdf

⁹¹ The FSA's recommended guidelines "Requirements for Primary Payment Service Providers": https://www.fi.ee/sites/default/files/2023-12/Finantsinspektsiooni%20soovituslik%20juhend%20N%C3%B5uded%20p%C3%B5himakseteenuste%20osutajatele_kinnitatud.pdf

The quality of reports submitted by credit institutions to the FIU has steadily increased from 2020 to 2024. In the first half of the assessment period, there were many reports that were weak in form and content, with suspicions being poorly substantiated. In recent years, the quality of reporting and the risk awareness reflected in the reports have improved: reports have become more targeted and justified, they are more clearly structured, and the formal quality (correctness of metadata and completeness of the submitted data) has also improved over time. However, progress among credit institutions has been uneven: some credit institutions stand out with strong analysis, while others continue to submit superficial or context-poor reports. The quality of reports and the extent of analysis have generally been positively influenced by the active use of the interbank information exchange channel (Salv Bridge⁹²).

In some cases, the FIU has had suspicions of defensive reporting. A more serious problem is the delay in reporting, as in cases of delay, the opportunities for the FIU and investigative authorities to intervene promptly are likely to be exhausted.

Compared to the reporting of other financial institutions and other sectors, the average level of reports from credit institutions is significantly better, the reports are more substantive and of greater use to the FIU. Most of the reports analyzed by the FIU and forwarded to law enforcement agencies come from credit institutions.

Cash transactions by clients are a money laundering risk factor that credit institutions take into account with due diligence. The proportion of cash amounts reflected in the reports of credit institutions out of the total amounts of transactions reported by this sector during the analyzed period ranged from 1% to 5% (see Table 29). Credit institutions have consistently been the most important reporters of suspicious cash transactions, while the cash-related reports from other obligated market participants have been overwhelmingly threshold-based (CTR-type reports, where credit institutions are the only sector that exceptionally does not have the obligation to submit them).

Table 29. Proportion of cash transactions in reports submitted by credit institutions to the FIU from 2020 to 2024

	2020	2021	2022	2023	2024
The amount of cash transactions in millions of euros	57.7	44.7	31.1	33.7	59.2
The amount of other transactions in millions of euros	4,159.5	864.2	1,180.8	1,262.5	1,523.2
The proportion of cash transactions in reports submitted by credit institutions	1%	5%	3%	3%	4%

Source: FIU

Adapting to the risk landscape and market dynamics remains crucial, requiring special flexibility and focus on relevant risks. To this end, the banking sector sees opportunities to promote practical cooperation, enabling market participants to learn from real cases and apply the lessons learned in their operations. The FSA and the FIU have offered corresponding opportunities for cooperation in the form of public and private sector cooperation forums. In the field of adopting and updating regulatory guidelines, market participants also see opportunities for even more proactive information exchange to ensure adequate preparation for future changes.

⁹² Salv Bridge is a network for combating financial crime based on cooperation between banks and fintech companies, through which financial institutions can exchange and enhance data on suspicious activities. <https://salv.com/product/salv-bridge/>

Credit institutions must also pay attention to the following typologies, which are difficult for market participants in the banking sector to identify, meaning there is uneven diligence and awareness of money laundering risks among market participants:

- A credit institution provides services within a correspondent relationship to another financial institution with weaker control systems and awareness, where the information underlying the payments is presented to the credit institution via batched payment files. In such cases, the risks of the respondent institution and the risk profile of its clients may not be adequately assessed.
- A credit institution offers VIBAN services to another financial institution, failing to adequately assess the risks of the financial institution and the risk profile of its clients.
- A client of the credit institution, after establishing a business relationship, begins to engage covertly in activities not declared to the bank at the time of establishing the relationship, for which they do not have a license, which do not match the bank's risk appetite, or which have a higher level of money laundering risk – for example, the client covertly provides investment services or trust and company services, or engages in peer-to-peer virtual currency exchange services.
- There is a specific circumstance arising from the local jurisdiction that the credit institution has not sufficiently considered when building its compliance framework, and therefore cannot identify the risk or suspicion:
 - o A non-profit organization that is a client of the credit institution is established by an e-resident who has negative media coverage related to terrorist financing and whose e-resident digital ID has been revoked by the PBGB.
 - o A private client of the credit institution transfers assets to the prepayment account of the TCB from a higher-risk third country from the bank account of a company engaged in a riskier activity (which is not a client of an Estonian credit institution).
- A credit institution has identified and assessed the money laundering risks of the ultimate beneficial owner of a non-resident company with a complex ownership structure but has failed to consider the risk of terrorist financing or the risk of sanctions evasion, meaning the credit institution does not have a comprehensive overview of the different risk levels of the client.

In the credit institutions' sector, it is still necessary to:

- Ensure an appropriate culture of money laundering risk management by the management of the credit institution.
- Provide sufficient resources and necessary authority to compliance functions within the organization.
- Improve technological solutions and enhance employee skills to identify suspicious transactions and ensure the quality and timeliness of reports.
- Provide feedback on the reporting of suspicious transactions, including communication on what happened after the reported incident.
- Ensure the operational availability of information on the revocation of e-resident digital IDs by the PBGB to the entire sector.

4.4. The Investment Sector

4.4.1. Investment firms

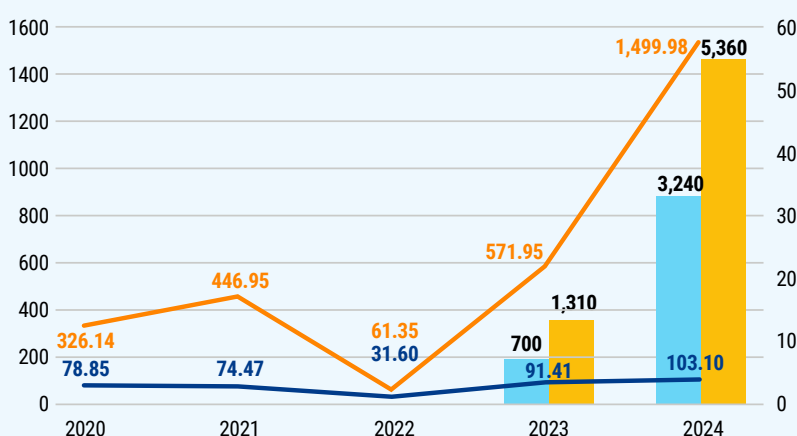
The level of vulnerability to money laundering for investment firms is **medium**.

By the end of 2024, there were eight investment firms and one branch of an investment firm registered in the European Union operating in Estonia. During the assessment period, the assets of clients in the investment firm sector grew nearly fourfold, but the market share of the value of investments compared to credit institutions and fund managers was still only 4.4% at the end of 2024. By the end of 2024, the two largest market participants were established during the assessment period, and they have significantly changed the nature of the entire investment firm sector through pan-European service provision, which has brought in a larger number of clients, including non-residents, a higher volume of transactions and assets held, and also better capabilities to contribute to anti-money laundering efforts.

In 2020, investment firms provided services worth 405 million euros, and by 2024, the volume of services increased to 1.603 billion euros. The activities of investment firms are mainly focused on the execution of orders related to securities and the provision of related securities custody services, which accounted for 94% of all services by the end of 2024. Retail investor trading through Estonian investment firms has grown rapidly since 2023, and the total turnover of securities transactions for all clients reached 8.6 billion euros in 2024.

Figure 7.
Volume of services provided by investment firms to clients based on the balance of instruments and the debit and credit turnovers of securities transactions, in millions of euros

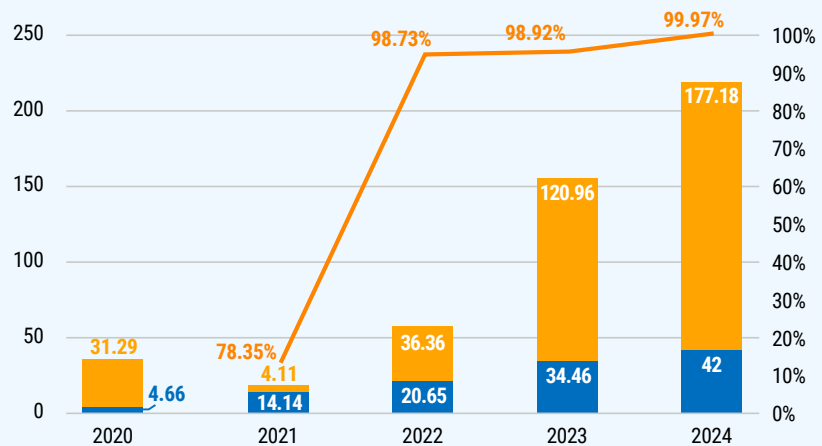
- Credit turnover of securities transactions
- Debit turnover of securities transactions
- Securities custody service (balance)
- Total other services (balance)



As of December 31, 2024, investment firms had 219,000 clients, of which 19% were residents and 81% were non-residents. Clients who were residents of the European Economic Area, the United Kingdom, and Switzerland accounted for over 99% of non-resident clients, and there were no clients from Belarus and Russia in the client bases of investment firms. Of all clients, 94% were individuals and 6% were legal entities, while among non-resident clients, 97% were individuals and 3% were legal entities. The risk structure of non-resident clients has become lower compared to the previous NRA period.

Figure 8.
Number of clients
of investment firms
in thousands

■ Number of non-resident clients
■ Number of resident clients
— The proportion of non-resident clients from the European Economic Area, the United Kingdom, and Switzerland among non-resident clients



During the assessment period, significant violations were identified in a few market participants regarding both anti-money laundering and other requirements. The FSA responded by restricting the provision of investment services, which led these market participants to reorganize their activities and relinquish their licenses. Considering the already small number of investment firms, the serious problems of the departing market participants negatively affected the overall vulnerability assessment of the investment firm sector.

The regulations applicable to investment firms are of a high standard. In addition to EU-wide legal norms, the country has also established local laws that comply with international standards (MLTFPA, VPTS). Certain obligations are specified at the legislative level, such as requirements for organizing compliance control and risk management within the organization, which strengthen the effectiveness of the sector's risk management measures.

The entry control system in the investment firm sector operates effectively. The FSA thoroughly analyzes the data submitted by companies and the suitability of their managers for the financial sector. Sector representatives highly value the FSA's ability to conduct risk-based supervision and believe that the supervisory authority has sufficient resources for this.

Compared to the previous NRA period, awareness of money laundering risks in the sector has improved. Investments in the development of monitoring solutions have significantly increased, and the number of employees in the anti-money laundering field has grown. Sector representatives also highlighted more frequent training of employees. Thanks to improved resources, the ability of investment firms to monitor their clients' activities has increased. This is reflected, among other things, in the increase in the number of reports submitted to the FIU during the assessment period (2020: 8 reports; 2024: 300 reports) and the improvement in their quality. However, only half of the investment firms submitted reports to the FIU during the assessment period. A significant portion of the sector's reports comes from one market participant, whose suspicions mainly concern transactions and clients outside Estonia.

A vulnerability-raising drawback in the investment firm sector is ensuring the separation of functions and controls within the organization across lines of defense. Attention is needed for the substantive updating of risk assessments and internal rules, as well as the quality and regularity of reports submitted to the board by the compliance control function. Also, circumstances related to the application of due diligence measures, such as identifying politically exposed persons, ultimate beneficial owners, and the origin of assets, need improvement. Considering that cross-border service provision has significantly increased and services are provided to non-resident clients, the vulnerability level is also raised by the fact that due diligence measures and/or transactions are carried out without face-to-face meetings with the client.

Considering the rapid and continuous growth of the investment firm sector, it is important to:

- Ensure that risk management and internal control measures keep pace with the rapid growth of companies.
- Effectively implement the know-your-customer principle.

4.4.2. Fund managers and management of voluntary pension funds

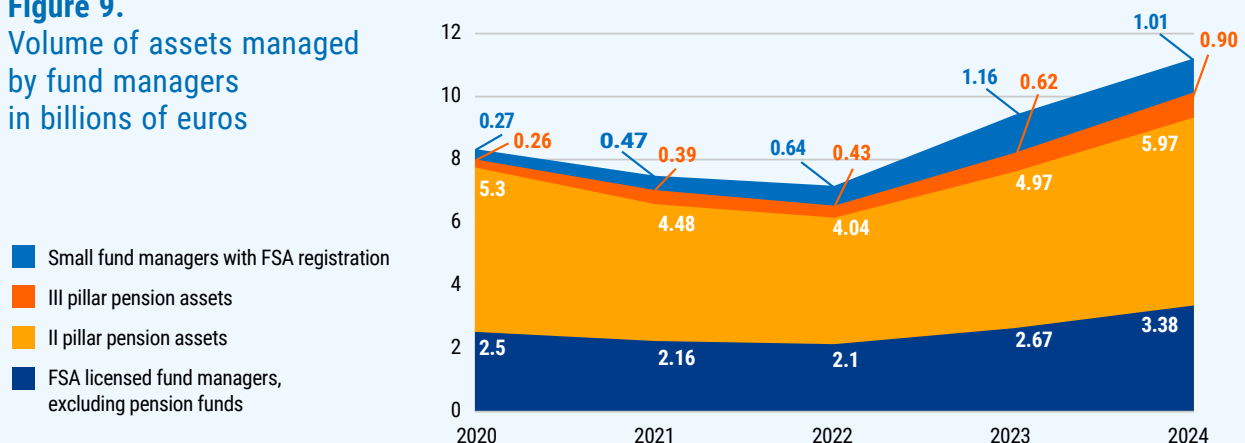
The level of vulnerability to money laundering for **fund managers** is **higher than average**.

Due to the fact that part of the sector operates under the license of the FSA and another part under the license of the FIU, it has been challenging to provide a uniform assessment for the sector as a whole. Despite providing similar services, fund managers are subject to partially different regulatory requirements, the intensity of supervision varies, and consequently, the information on the effectiveness of fund managers' risk management solutions differs.

A significant portion of the activities of fund managers is based on pension funds, where mandatory and voluntary funds differ in terms of funding methods, asset origin assessment, cash flow management, and payout procedures. Therefore, the vulnerability level related to the management of **voluntary pension funds** was assessed separately, which is **lower than average**.

Due to the exclusion stipulated in § 6 (2) 6 of the MLTFPA, **no assessment was given** for the management of **mandatory pension funds**. To obtain an accurate result, the volumes of services related to mandatory pension funds, which constitute the majority of market participants' activities, were excluded from the assessment of both modules. The volume of assets managed by fund managers was 11.26 billion euros at the end of 2024, of which 61% were pension fund assets (5.97 billion euros mandatory and 0.9 billion euros voluntary pension funds), 30% were assets of fund managers with an FSA license managing funds other than pension funds, and 9% were assets of fund managers with a FIU license.

Figure 9.
Volume of assets managed
by fund managers
in billions of euros



Fund Managers

At the end of the observed period, 12 fund managers and six small fund managers operating in Estonia had licenses issued by the FSA for managing public funds. The volume of client assets managed in equity funds was 209.6 million euros in 2020, but after a significant decline in 2021, it remained at 98.9 million euros by 2024. The volume of client assets held in real estate funds has shown a steady increase, growing from 207.8 million euros in 2020 to 358.6 million euros in 2024. Among the aforementioned, local pension fund assets are also invested in Estonian public funds.

By the end of the assessment period, 81 small fund managers engaged in managing non-public funds were registered with the FSA under § 453 (1) of the Investment Funds Act (IFS), requiring a license from the FIU to provide services, but not all of them have applied for the required license. During the assessment period, 67 such financial institutions held a FIU license, providing small fund manager services as a sub-service⁹³. Some fund managers with a FSA license have not registered their activities with the FSA and do not fulfill the reporting obligations arising from the IFS.

The number of small fund managers with a FIU license increased significantly during the assessment period: over four-fifths of market participants entered the market in 2020 or later. More license and registration applications were submitted during the assessment period, but the entry controls of the two supervisory authorities rejected some of them. According to statistics submitted to the Financial Supervision Authority, the volume of client assets managed by small fund managers operating under a FIU license increased significantly during the assessment period: from 367 million euros in 2020 to 1.056 billion euros by the end of 2024. Data collected through the FIU remote control questionnaire shows that by the end of 2023, 94% of the client assets managed by fund managers operating under a FIU license belonged to legal entities, and more than half (54%) of the managed assets were held by clients with non-resident beneficial owners.

Considering the rapid growth in the number of market participants and associated risks, several regulatory changes were made to the IFS, giving the FSA the right to reject a registration application or delete it from the register under certain conditions. Since the FSA has more legal grounds to reject an application than the FIU, the FIU requires registration with the FSA as a prerequisite for processing a license application. For the FIU, a bottleneck in market regulation is the limited ability to revoke the licenses of inactive market participants or those who do not update their data. This is a broader issue affecting the vulnerability of all financial institutions under FIU supervision. Additionally, problems arise from conducting supervisory actions only concerning small fund managers registered with the FSA and the lack of access to reports submitted by small fund managers to the FSA. Although the effectiveness of the entry controls of the two supervisory authorities was assessed as effective for small fund managers, the emerging issues indicate that the parallel obligation to register and submit data to the FSA and apply for a license from the FIU creates double administrative burdens for market participants and may not be justified from a supervisory perspective.

The effectiveness of entry controls for public fund managers and the efficiency and risk-based nature of supervision were highly rated.

In the fund management sector, there are market participants who require additional training on anti-money laundering (AML) requirements and their implementation. Supervisory activities have identified deficiencies in risk management solutions and the application of due diligence measures. During supervisory inspections of

⁹³ Not all service providers who have or have had a financial institution license have defined the sub-services they offer in the Economic Activities Register. Based on the responses to the remote control questionnaire conducted in the sector in the spring of 2024, the FIU also found that only about two-thirds of the registered service providers actually offer services, and many have not updated their data, including information on sub-services, in the register. According to the remote control mapping, 52 supervisory subjects provided fund management services in 2024.

FIU-supervised entities, it was found that a quarter of small fund managers with a FIU license do not update their risk appetite, risk assessment, and procedural rules documents with sufficient diligence. Nearly half of the companies do not have the person responsible for AML provide written reports to the board, and few conduct audits in the AML field. Additionally, it was revealed that more than a third of market participants do not regularly offer AML training to their employees. Although more than a quarter of small fund managers under FIU supervision served politically exposed persons (PEPs) or their close associates, nearly half of these service providers did not apply enhanced due diligence measures to PEP clients.

Compared to the previous NRA period, the awareness of money laundering risks in the sector has not significantly improved. Fund managers have been passive in reporting suspicious transactions: during the assessment period, only seven market participants submitted reports to the FIU, and only a few reports were submitted. Considering the volume of assets in the sector, the large number of service providers, and the international clientele, the reporting by fund managers is likely not in line with the inherent money laundering risk of the investment sector and indicates a general low risk awareness among market participants.

For fund managers, it is important to manage risks by:

- Aligning the company's risk management solutions with applicable anti-money laundering (AML) requirements, particularly by regularly updating procedural rules, risk appetite, and risk assessment documents according to the specific company's profile and the surrounding risk environment.
- Paying attention to knowing their clients (including PEP clients and their close associates) and identifying the origin of clients' assets.
- Improving awareness of sector-specific money laundering risks through training.
- Enhancing the quality of reports submitted to the FIU.

Management of Voluntary Pension Funds

During the assessment period, five fund managers managed the assets of 17 voluntary pension funds, four of which are associated with local banking groups. The volume of assets in voluntary pension funds was 255 million euros at the end of 2020, which had grown to 896 million euros by the end of 2024.

Market participants offering voluntary pension fund management services are mostly associated with banking groups, and the obligations related to the application of due diligence measures are largely delegated within the group. This has led to better awareness of money laundering risks, as training is conducted across the group, and since standards in credit institutions are stricter than the financial sector average, this also pressures fund managers to comply with AML requirements.

The low number of suspicious transaction reports is due to the nature of the lower-risk product, with incoming payments being smaller, regular, and easier to understand compared to other fund contributions.

According to market participants, certain problems have arisen in the application of due diligence measures since 2018, when all transactions related to pension fund units were transferred to the pension register under the Pension Center⁹⁴. This change, among other things, gave clients the ability to independently switch products or contracts at any time, and fund managers essentially lack the means to refuse to accept a client. Market participants also see a problem with the limitation of terminating business relationships with clients in the

⁹⁴ The Pension Register is a state information system database for registering the units of mandatory (second pillar) and voluntary (third pillar) pension funds and the transactions related to them, as stipulated in the Pension Funds Act.

context of voluntary pension fund products – while it is possible to freeze clients’ assets and stop additional contributions when financial sanctions are applied, the legal grounds for terminating a business relationship with a client are limited. Considering the inherently lower risk level of the product, market participants deem it important to establish a simplifying exception for voluntary pension funds in the regulation of relying on the due diligence measures applied by another obliged entity as regulated in § 24 of the MLTFPA.

In managing voluntary pension funds, fund managers **must still pay attention to identifying the origin of assets**, including payments received from third parties.

4.5. Life Insurance Sector

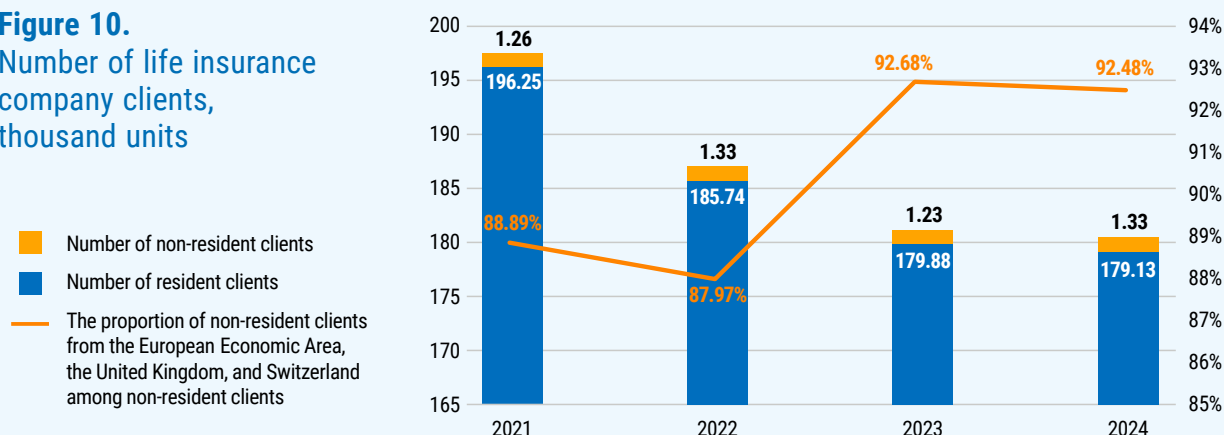
The level of money laundering vulnerability in the life insurance sector is **low**.

In Estonia, life insurance is offered by five life insurers, two of which have Estonian licenses and three are European Economic Area life insurers operating through Estonian branches. Approximately 70% of the sector belongs to the same group as credit institutions. During the assessment period, the total number of market participants remained the same, but there were changes in the structure of market participants when one branch ceased operations, transferring its Estonian business (insurance portfolio) to another branch established in Estonia.

Life insurers use both insurance brokers and agents to market life insurance, with agents mainly being credit institutions belonging to the same group. During the assessment period, a total of 12 insurance brokers mediated life insurance contracts, with the volume of life insurance premiums collected by them amounting to only 1% of the total life insurance premiums as of 2024, and no investment risk life insurance contracts were mediated.

As of the end of 2024, 99.92% of the 180,500 life insurance clients were individuals, with 99.27% of them being Estonian residents. The share of resident individual clients has remained above 99% throughout the assessment period.

Figure 10.
Number of life insurance company clients, thousand units



The volume of life insurance premiums was 85.6 million euros in 2020 and recovered from an interim decline from 79.4 million euros in 2022 to 84 million euros in 2024. In terms of products considered higher risk in the assessment of money laundering vulnerability, both investment risk life insurance and capital accumulation insurance volumes were in a downward trend. The volume of investment risk life insurance premiums decreased from 34 million euros in 2020 to 30 million euros in 2024, and the volume of capital accumulation insurance premiums fell from 10 million euros in 2020 to 6 million euros in 2024.

Table 30. Life insurance premiums, thousand euros

Type of Insurance	2020	2021	2022	2023	2024
Investment risk life insurance	33,953	39,338	30,943	30,480	29,917
Capital accumulation insurance	9,841	8,889	8,010	7,015	6,033
Additional insurance	8,876	10,645	13,465	17,149	18,515
Birth and marriage insurance	1	0	0	0	0
Pension insurance	12,039	8,836	6,622	7,631	6,536
Death insurance	20,850	19,171	20,402	21,715	23,016
Other life insurances	0	0	0	0	0
Total insurance premiums received	85,560	86,879	79,442	83,989	84,017

Source: Statistics Estonia, RRI05

There was no similar stability in insurance claim payments, with the peak of the assessment period in 2023, when payments amounted to 133.2 million euros – in 2024, it was 71.3 million euros. The products that significantly influenced the 2023 payments were investment risk life insurance payouts, which reached 91.8 million euros, while in 2024, the payouts were more comparable to the usual: 32.7 million euros. Capital accumulation insurance payments also peaked in 2023, with 20.8 million euros paid out, while in 2024, insurance claims were compensated for 15.4 million euros.

Table 31. Life insurance claim payments in thousands of euros

Type of Insurance	2020	2021	2022	2023	2024
Investment risk life insurance	29,312	32,607	51,675	91,768	32,748
Capital accumulation insurance	16,621	17,697	16,374	20,787	15,381
Additional insurance	1,781	2,776	4,277	5,789	6,514
Birth and marriage insurance	0	12	6	1	0
Pension insurance	12,739	55,461	21,346	12,385	12,822
Death insurance	2,730	3,342	2,678	2,495	3,825
Other life insurances	0	0	0	0	0
Total insurance premiums received	63,183	111,894	96,355	133,226	71,290

Source: Statistics Estonia, RRI05

The analysis of the life insurance sector confirmed that the field is well-regulated (MLTFDPA, Insurance Service Act) in accordance with the European Union legal framework and international standards. The sector-specific requirements applicable to life insurers also help strengthen the effectiveness of money laundering risk management measures (such as additional training requirements and the organization of the compliance control function).

The entry control system in the life insurance sector operates effectively, relying on a strong legal framework. Employees and managers demonstrate a high level of commitment to integrity and reliability, and the key person suitability assessment system functions properly. The effectiveness of supervisory procedures was also rated highly, which was partly due to the application of the risk-based supervision principle.

The sector's awareness of money laundering risks is at a high level, considering the data on training conducted and the quality of risk assessments. The effectiveness of the compliance control function has improved, although minor deficiencies in the application of due diligence measures were identified.

The supervision of suspicious transactions in the life insurance sector operates effectively. Some life insurers belong to banking groups, which has allowed the delegation of due diligence measures within the group. This provides a good overview of the entire client's activities across services and, in addition to the sector's low risk level, explains the low number of suspicious reports submitted to the FIU. No money laundering cases related to the life insurance sector have been identified in Estonia. The issues related to the availability of beneficial owner information do not have a significant impact on the life insurance sector, as the proportion of legal entity clients is almost negligible.

In the life insurance sector, it remains important to:

- Ensure that life insurers pay attention to knowing their clients and identifying the origin of their assets, as well as applying due diligence measures to insurance premium recipients.
- When relying on data collected by another obliged entity and delegating the application of due diligence measures, ensure that the life insurer has complied with the requirements set out in § 24 of the MLTFPA.
- Ensure that insurance brokers fulfill their obligations under the MLTFPA to apply due diligence measures to clients when mediating life insurance contracts.

4.6. Other Financial Services

4.6.1. Payment institutions and e-money institutions

The level of money laundering vulnerability for payment institutions and e-money institutions is **medium**.

At the beginning of the assessment period, there were 12 payment institutions, one branch of a payment institution registered in another European Economic Area country, and one e-money institution registered in Estonia. By the end of 2024, there were 14 payment institutions, two branches of payment institutions registered in other European countries, and three e-money institutions registered in Estonia.

Although new e-money institutions have entered the market, the activities of market participants during the assessment period have largely been in the preparatory phase, and therefore the volumes of these service providers constitute a small part of the total transaction volume of the sector. Consequently, e-money institutions and their services were not assessed separately but were evaluated together with other payment services offered by payment institutions.

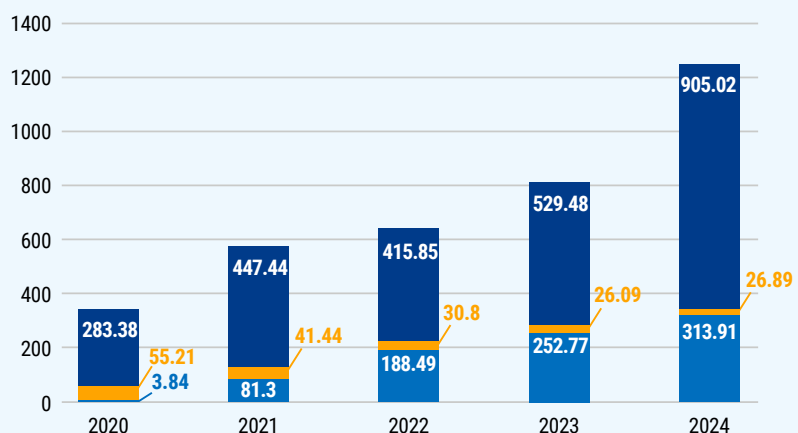
In the national risk assessment, three types of payment services were distinguished in the sector: 1) payment initiation service, 2) money transfer, and 3) other payment services (including services related to payment accounts, issuance of payment instruments, and acceptance of payment transactions).

During the assessment period, significant changes occurred in the transaction volumes of the sector, the share of service types, the distribution of market shares, and the client portfolio of market participants. The volume of payments in the sector increased more than threefold during the assessment period – from 342 million euros to 1.2 billion euros. Despite this, in 2024, the payments of the payment institutions and e-money institutions sector accounted for 0.25% of the total payments in the financial sector.

Among the types of services, other payment services have grown the most in volume. While the volume of these services was 283.4 million euros in 2020 (83% of the sector’s total volume), by 2024, the volume of services reached 905 million euros (73% of the sector’s total volume). Conversely, the volume of the payment initiation service has seen the largest proportional growth in the sector. While the volume of the service was 3.8 million euros in 2020 (1% of the sector’s total volume), by 2024, it was 313.9 million euros (25% of the sector’s total volume). Considering that service providers operating in the Estonian market also operate under licenses issued in other European Union member states, the growth of the service has been even greater in terms of both volume and sector share. In contrast to the growth of payment initiation and other payment services, the volume of money transfer services has significantly decreased. While money transfer services were provided to the extent of 55.2 million euros in 2020 (16% of the sector’s total volume), in 2024, it was 26.9 million euros (2% of the sector’s total volume).

Figure 11.
Turnover of payment transactions by payment institutions and e-money institutions by type of payment service, million euros

- Payment initiation service
- Money transfer
- Other payment service



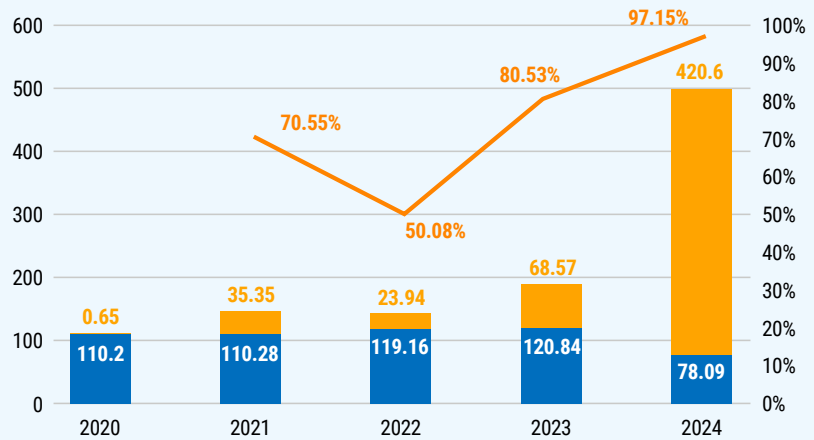
In connection with the above, it is noteworthy that there has been a concentration in the distribution of market shares in the sector, and as a result of the changes, the market share of the two largest payment institutions accounts for 78% of the sector’s volume. The increase in market shares is primarily due to the rapid growth of market participants’ activities in other European Economic Area countries and the United Kingdom.

As a result, there has also been a significant change in the structure of payment transactions. While domestic payment transactions accounted for 80% of the sector’s transaction volumes in 2020, by 2024, the share of domestic payments was 33%. At the same time, the share of foreign payments has significantly increased, accounting for 9% of the sector’s payments in 2020, but 59% in 2024. The share of cross-border payment transactions has remained at a similar level during the observed period.

The change in the structure of payments has also led to an increase in the proportion of non-resident clients. As of the end of 2024, the sector’s market participants had a total of 499,000 clients, of which 16% were Estonian residents and 84% were non-residents. Of the non-resident clients, 97% were residents of European Economic Area countries and the United Kingdom.

Figure 12.
Number of clients of payment institutions and e-money institutions, thousand units

- Non-residents
- Residents
- The proportion of non-resident clients from the European Economic Area, the United Kingdom, and Switzerland among non-resident clients

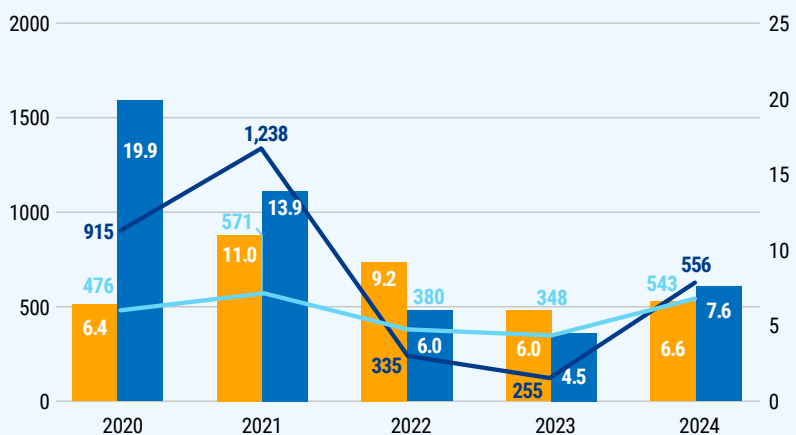


The described changes as a whole affect the risks and vulnerabilities associated with the sector. Alongside the decrease in the volume of money transfer services, the volume of cash transactions has also decreased, reducing the sector’s vulnerability related to cash transactions. In their place, technology-based payment solutions have emerged in the sector. Considering that a large part of the transactions are cross-border and services are provided to non-resident clients, the vulnerability is also influenced by the fact that due diligence measures and/or transactions are carried out without face-to-face meetings with the client. These vulnerabilities can create a favorable ground for market participants to commit fraud from a risk perspective.

Reports on money transfers submitted to the FIU by foreign payment institutions and their payment agents operating in Estonia were still very important in the FIU’s information concerning payment and e-money institutions during the national risk assessment period (Figure 13). Since these market participants are not under the supervision of the FSA but operate in the local financial environment, additional vulnerabilities may arise from these service providers. It is important to be aware of this, but in the context of this risk assessment, the vulnerabilities associated with cross-border service providers and their agents cannot be attributed to local market participants, except when they serve them.

Figure 13.
Number of reports submitted by payment and e-money institutions and their payment agents, and the amounts associated with the reports in 2020–2024

- Amount related to reports from cross-border service providers (mln EUR)
- Amount related to reports from Estonian service providers (mln EUR)
- Number of reports from Estonian service providers
- Number of reports from cross-border service providers



The vulnerability level of the payment institutions sector is primarily reduced by high entry requirements and, on the other hand, by effective, consistent, and risk-based supervisory activities. This includes the FSA having a complete overview of the activities of agents operating abroad for Estonian payment institutions.

In the payment institutions and e-money institutions sector, it is necessary to manage money laundering risks by:

- Ensuring that the management of payment institutions fosters an appropriate culture of money laundering risk management.
- Enhancing technological solutions and improving employees' skills in detecting suspicious transactions, as well as ensuring the quality and timely preparation of reports.

4.6.2. Currency exchange service providers

The level of money laundering vulnerability for currency exchange service providers is **below average**.

According to the information collected during the risk assessment, the currency exchange sector has a small significance in the context of the national financial system, which influenced the vulnerability level to be lower than average.

At the beginning of the assessment period, 82 currency exchange service licenses had been issued in Estonia, but by the end of 2024, this number had decreased to 23. The significant decrease in the number of licenses was partly due to the COVID-19 pandemic that began in 2020, forcing many service providers to cease operations (55 service providers between 2020 and 2021). On the other hand, the market was also regulated by the activities of the FIU. During the sector-wide data collection conducted in 2024, it was found that many licensed service providers either no longer provide services or do not purchase physical currency exchange services, and 14 market participants relinquished their licenses.

Despite the fact that there were 23 valid licenses registered by the end of 2024, only up to ten market participants were actively operating in the sector at that time. Based on the collected information, the volume of currency exchange transactions in the sector is up to 100 million euros per year⁹⁵. Considering the significant downward trend in the number of market participants and the additional cash transaction limiting legal norms coming into force in 2027, the sector's volume is likely to decrease further in the coming years.

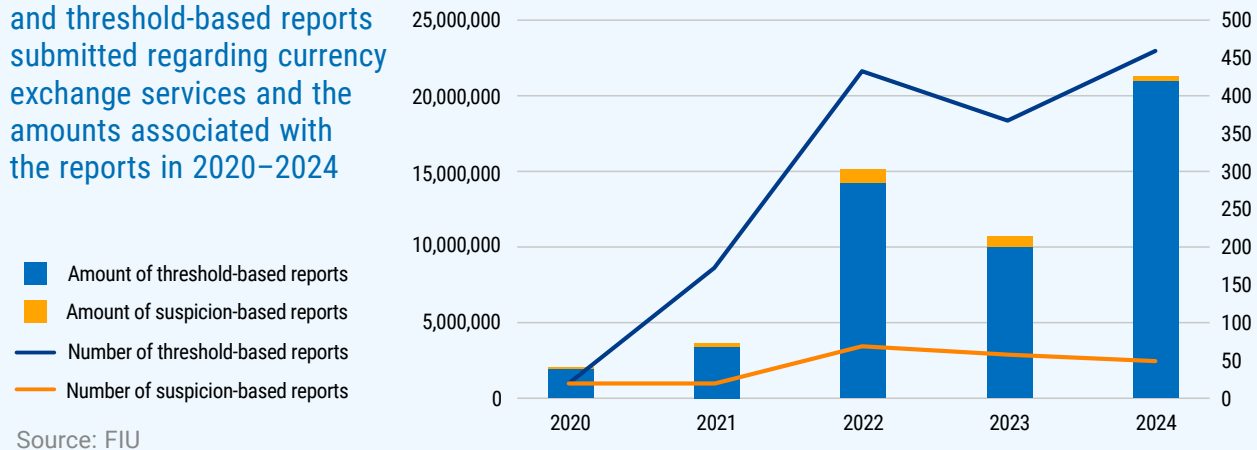
The volume of currency exchange services offered by market participants and the size of the organization vary significantly, which means that the vulnerabilities associated with market participants in the sector are also different. Some market participants offer currency exchange services only as a small-scale ancillary activity. Larger market participants have relatively good awareness of the obligations set by law and use technological solutions in the application of due diligence measures and transaction execution, while smaller service providers have less awareness and more limited opportunities to use the relevant systems and solutions.

Between 2020 and 2024, six currency exchange service providers submitted reports to the FIU. The reporting by currency exchange service providers is of very different quality, but the common feature is overwhelmingly threshold-based rather than suspicion-based reporting. In 2024, the share of CTR reports in all sector reports was 90%, and the total amount associated with the reports was 99%. Since 2022, the amounts associated with the reports have increased significantly due to threshold-based reports (2021: 3.8 million euros, 2022: 15.2

⁹⁵ Although exact data on the transaction volumes of market participants were not collected during the assessment period, this is indicated by public data on the activities of licensed companies, notifications sent to the FIU, as well as interviews conducted and responses to questionnaires sent to market participants during the risk assessment process.

million euros, 2023: 10.8 million euros, 2024: 21.4 million euros), meaning that large individual transactions or regular cash transactions by individuals have increased significantly. At the same time, the share of suspicion-based reports in the sector has decreased.

Figure 14.
Number of suspicion-based and threshold-based reports submitted regarding currency exchange services and the amounts associated with the reports in 2020–2024



The sector’s risks have been significantly impacted by the full-scale war between Ukraine and Russia, resulting in a large influx of war refugees to Estonia, as well as other third-country residents who wish to exchange the foreign currency they brought with them into euros. Transactions may occur as a single large transaction or be structured into smaller transactions, including those below the identification threshold. Additionally, service providers face increased risks due to trade sanctions imposed on Russia and Belarus and the export ban on euros and other EU member state currencies.

For currency exchange service providers, it is important to:

- Improve awareness of money laundering risks and the applicable requirements in the field of anti-money laundering through training.
- Enhance the quality of reports submitted to the FIU.

4.6.3. Savings and loan associations

The level of vulnerability to money laundering for savings and loan associations is **medium**.

In the entire loan market, loans issued by savings and loan associations accounted for less than 0.3%, and the deposits of union members made up about 0.3% of the total deposits in Estonia.

The savings and loan associations’ market in Estonia has contracted during the assessment period. The most noticeable change has been the decline in market participants: of the 26 savings and loan associations operating at the beginning of the period, 12 had ceased operations by the end of 2024 and were either deregistered, bankrupt, or in liquidation.

By the end of 2024, 12 savings and loan associations had a financial institution license from the FIU, and two operated under a payment institution license from the FSA. According to the FIU, only eight savings

and loan associations showed signs of active service provision. A significant issue in the savings and loan associations' market is the potential for unlicensed operations: during the assessment, three named savings and loan associations were found to lack the required license to offer services.

The number of credit union members has decreased at a slower pace than the number of service providers: from 15,600 members at the end of 2020 to less than 13,100 members at the end of 2024. By the end of the assessment period, the balance of associations members' deposits was 106 million euros, which constituted only 0.3% of the total deposits in Estonia (32,102.6 million euros). The balance of loans issued by savings and loan associations (110.4 million euros) was on a slight downward trend by the end of the assessment period. The majority of the loan balance consisted of loans to companies, particularly real estate companies.

The main money laundering risk associated with savings and loan associations during the assessment period stemmed from the activities of the associations leaders, who used savings and loan associations as a means to commit predicate offenses, rather than from the activities of clients using the savings and loan association for money laundering purposes. The assessment period included one active money laundering case involving the actions of a savings and loan association board. During the period under review, criminal proceedings were conducted against the management of three associations for investment fraud or embezzlement. The criminal exploitation of savings and loan associations has damaged trust in the financial sector, and the cases have caused significant harm to vulnerable groups in society, such as the elderly. This indicates that it is a problematic sub-sector requiring greater regulatory and supervisory intervention.

CASE:

At the beginning of the assessment period, the FIU observed several cases of credit union abuse, where funds collected from union members were moved out of the union through companies associated with the union's council or board members. The pattern of activity indicated embezzlement and subsequent money laundering. Companies associated with the governing body members often had unsubmitted reports for recent years, lacked actual economic activity, and legal entities were abandoned to front persons.⁹⁶

Savings and loan associations are subject to the requirements of the MLTFPA, but it became clear that regulatory improvements were needed (restructuring into cooperative banks) to ensure effective supervision of the activities of savings and loan associations and the protection of clients' assets.

The FIU and investigative authorities provided input for necessary regulatory changes based on cases under investigation in the early 2020s, including ensuring more effective supervision of the sector. The Ministry of Finance has developed a comprehensive package of changes to ensure the gradual transformation of savings and loan associations into more strongly regulated cooperative banks, but by the end of the assessment period, major changes had yet to come into force. During the assessment period, a union of savings and loan associations and a separate guarantee fund were established on the initiative of market participants, but only a few savings and loan associations belong to the professional union, which means that clients' assets still lack protection comparable to that of credit institutions.

⁹⁶ FIU Yearbook 2020, p. 32 https://fiu.ee/sites/default/files/documents/2021-06/rahapesu%20aastaraamat%202020%20est_2.pdf

4.6.4. Credit providers and intermediaries and other financial institutions

The level of vulnerability to money laundering for financial institutions engaged in credit provision and intermediation is **medium**.

As of December 31, 2024, there were 42 credit providers and seven credit intermediaries operating in Estonia. In addition, there were at least 80 market participants operating under a financial institution license issued by the FIU, offering various loan services (excluding consumer credit), leasing services, or guarantee and warranty transaction services. All of these were assessed in one module as financial institutions providing and intermediating credit (lenders). Less vulnerable are credit providers belonging to the same group as local credit institutions, which have a dominant share of the non-credit institution loan market. Higher vulnerability, but with a small share of the loan market, are market participants offering credit services to legal entities, whose financial supervision needs significant strengthening.

Some market participants operate under a crowdfunding service model, but these companies currently only have either a credit provider or intermediary license issued by the FSA or a financial institution license issued by the FIU.

In the field of anti-money laundering, the supervisory authorities that issued the respective licenses oversee the activities of lenders: the FSA oversees credit providers and intermediaries, while the FIU oversees financial institutions offering loans, leasing, guarantee, or warranty transaction services to legal entities. About 80% of the credit providers' market share belongs to credit providers that are part of the same group as local credit institutions. The market share of participants with a license from the FSA in the entire loan market, where credit institutions clearly dominate, was less than 5%. The market share of financial institutions offering various credit services under an FIU license in the entire loan market was just over one percent (1.2%).

The volume of consumer credit issued by credit providers has grown from 1.18 billion euros in 2020 to 1.52 billion euros in 2024, but it still accounts for less than 4% of the entire consumer credit market. The balance of leasing services provided by credit providers and intermediaries increased from 0.80 billion euros to 0.98 billion euros during the assessment period, but still accounted for only 2% of the total loan market balance.

The balance of loans, leases, and factoring issued by FIU-supervised entities was 0.41 billion euros, according to data collected by the FIU. The leasing balance of leasing providers with an FIU license (73 million euros at the end of 2023) accounted for less than 0.2% of the entire leasing market.

Detailed data on market participants under FIU supervision is only available as of the end of 2023, which the FIU collected from supervised entities in the spring of 2024 through a remote control questionnaire. Data necessary for risk assessment covering the entire assessment period is lacking because financial institutions with an FIU license are not subject to regular reporting.

The FIU's remote control led to a decrease in passive license holders: while there were at least 101 financial institutions providing loan services during the assessment period, their number fell to 80 by the end of the period, according to MTR data. It also became clear that there are significantly more financial institutions providing loan services than reflected in the MTR. Many companies that applied for a license in the previous decade have left the sub-services provided unspecified and have not updated their data. The current MLTFPA does not require a change of license application and document update when the sub-sector changes. Additionally, the FIU identified several financial institutions with an FIU license that offer services to consumers and therefore require a license from the FSA.

Financial institution licenses are often applied for by non-residents, where the company's only connection to Estonia is a legal entity in Estonia and a contact person working in Estonia. Unlike the licensing requirements for virtual currency service providers, the FIU does not have the option to refuse a financial institution license if the company's place of business is not Estonia. Licensing financial companies operating outside Estonia may increase the sector's money laundering risk level.

The FSA has conducted remote controls and thematic on-site inspections on a risk-based basis for credit providers and intermediaries. Although certain deficiencies have been identified during supervisory activities (mainly in risk assessment, internal rules, and the application of due diligence measures), the overall quality of risk management and compliance control functions of these market participants can be considered good.

Both the FSA and the FIU have identified that many market participants offering loan or leasing services have failed to update their procedural rules or risk appetite and risk assessment documents despite changes in the risk environment. The FIU has most frequently identified deficiencies in the application of due diligence measures. Although some market participants use technological solutions for due diligence and transactions, many service providers are very small companies with weak or virtually non-existent systems and monitoring solutions. The commitment of management to anti-money laundering efforts is also noticeably lacking among lenders, which in turn has affected the inadequate training of employees involved in anti-money laundering and has led to relatively low risk awareness and compliance with reporting obligations.

During the assessment period, a total of 33 loan market participants, or 25% of market participants, submitted reports to the FIU. The reports are generally low in content, often related to fraud cases or unspecified suspicions. The FIU has rarely used reports from the loan sector in information transmissions to investigative authorities. Within the loan sector, the least reporting group is leasing providers, from whom the FIU received only a few reports during the assessment period. The FIU has observed that loan market participants more frequently appear in suspicious information submitted by various reporters compared to other financial institutions. This indicates deficiencies in information collection, anti-money laundering awareness among lenders, compliance control systems, and compliance with reporting obligations, which significantly affect the overall vulnerability of the sector.

Lenders operating mainly through web platforms have proven to be quite vulnerable to various online frauds and transactions using stolen identities. Fraud schemes have become more frequent and increasingly sophisticated during the assessment period. Therefore, **it is important to pay attention to the application of due diligence measures to clients, especially non-residents when providing cross-border services.**

To mitigate risks in the sector, it is also important to:

- Improve awareness of money laundering risks and applicable requirements through training.
- Ensure the verification of the connection between the payer and the borrower for loan repayments received from third parties.
- Improve the quality of reports submitted to the FIU.

5. ML Vulnerabilities of DNFBPs

According to the MLTFPA, obligated entities also include various non-financial companies and professions⁹⁷, such as gambling organizers, real estate transaction intermediaries, wholesale dealers of precious metals, accountants and tax advisors, auditors, pawnshops, corporate service providers, and other traders (in the case of larger cash transactions). Additionally, notaries, lawyers, bailiffs, bankruptcy trustees, and other legal service providers must fulfill obligations arising from the MLTFPA when conducting certain transactions.

Table 32. Sectors assessed in the field of designated non-financial businesses and professions or DNFBPs

DNFBPs sector participants	Supervisory authority	Number of participants as of 31.12.2024	Obligated entities by MLTFPA § 2 (1) and (2)	Threat	Vulnerability
Gambling organisers	FIU, TCB	42	all	Above average	Above average
Dealers in precious metals	FIU	94	all	Below average	Medium
Traders	FIU	n/a	conditional	Below average	High
Pawnshops	FIU	100	all	Low	Medium
Auditors	FIU	337	all	Low	Below average
Other legal service providers	FIU	ca 800	conditional	Low	Medium
Bailiffs	FIU	39	conditional	Low	Below average
Bankruptcy trustees	FIU	61	conditional		
Accountants and tax advisors	FIU	ca 8,000	all	Medium	Medium
Real estate brokers	FIU	ca 1,000	all	Medium	Above average
Company service providers	FIU	259	all	Above average	Above average
Lawyers	Bar Association	1,154	conditional	Medium	Medium
Notaries	Chamber of Notaries	87	conditional	Medium	Medium

The assessments of money laundering vulnerability for DNFBPs are presented in more detail for all sectors in the following subsections.

⁹⁷ DNFBPs or designated non-financial businesses and professions.

A brief overview of the most significant money laundering threats⁹⁸ in the professional and freelance sector:

- Money laundering is a complex, multi-stage process that often involves **intermediaries or money laundering service providers**. These are individuals or companies that help conceal criminally derived assets for a fee. Their activities make it difficult to identify and confiscate criminal proceeds. In international criminal networks, **financial and legal advisors** play a key role.
- The gambling sector has a higher than average level of money laundering threat. **Remote gambling** and foreign service providers dominate the sector in terms of both volume and money laundering risks. According to international studies, the sector is increasingly associated with the movement of criminal money, and **online casinos** have a growing share in laundering criminal proceeds.
- Companies established in Estonia are still used for criminal purposes, especially in international organized crime. The risk level increases due to the extensive and easily accessible services offered by service providers, particularly to non-residents. Many companies that lack operations and bank accounts in Estonia are created through **company service providers** and are associated with money laundering and other crimes.

5.1. Description of the Methodology

Similar to the assessment of vulnerability in the financial sector (see pages 53–54 for more details), the vulnerability of DNFBPs, was also analyzed. Several World Bank assessment modules were used in the assessment of market participants in the DNFBPs sector (see Table 33).

Table 33. Modules used in the assessment of the DNFBPs sector

Market participants in the DNFBPs sector	Module used in the assessment
Gambling organisers	Module 7.B Vulnerability-Product Based
Dealers in precious metals	Module 7.A DNFBPs Vulnerability
Traders	Module 7.A DNFBPs Vulnerability
Pawnshops	Module 7.A DNFBPs Vulnerability
Auditors	Module 7.A DNFBPs Vulnerability
Other legal service providers	Module 7.A DNFBPs Vulnerability
Bailiffs and bankruptcy trustees	Module 7.A DNFBPs Vulnerability
Accountants and tax advisors	Module 7.A DNFBPs Vulnerability
Real estate brokers	Module 7.A DNFBPs Vulnerability
Company service providers	Module 7.C TCSP Vulnerability Add-on
Lawyers	Module 7.A DNFBPs Vulnerability
Notaries	Module 7.B Vulnerability-Product Based

⁹⁸ See for details Chapter 2.

Similar to the criteria for assessing the vulnerability of the financial sector, the working group for DNFBPs was evaluated based on 12 assessment criteria:

- The scope of the anti-money laundering legal framework,
- The effectiveness of supervisory activities,
- The existence and enforcement of administrative penalties,
- The existence and enforcement of criminal penalties,
- The existence and effectiveness of entry controls,
- The commitment of professional workers,
- Awareness of money laundering risks in the sector,
- The effectiveness of the compliance control function,
- The effectiveness of monitoring and reporting suspicious transactions,
- The availability and access to information on the beneficial owner,
- The availability of a reliable identification infrastructure,
- The availability of independent information sources.

The last three criteria were also assessed in the national vulnerability module, and therefore these topics were covered in more detail in the national vulnerability chapter.

Additional criteria for the assessment modules focused on product assessment include the profile of the product's customer base, the volume of cash usage, the involvement of intermediaries or agents, the anonymity of the product or service provision, and others.

5.2. Gambling Organizers

The vulnerability to money laundering for gambling organizers is **above average**.

Gambling in Estonia is regulated by the Gambling Act. To operate in the gambling sector, an activity and/or organization license is required, which is issued, refused, or revoked by TCB. **As of December 31, 2024, there were 42 licensed gambling organizers operating in the Estonian gambling market.** By the end of 2024, there were 47 organization licenses issued for casinos on land and ships, 29 for betting offices, and 37 organizers had a remote gambling⁹⁹ license.

Commercial lottery organizers, whose lottery prize fund value is up to 10,000 euros, and lottery organizers, whose lottery prize fund value is up to 1,000 euros, are not considered obligated entities. In Estonia, lotteries with a prize fund value of over 1,000 euros that are not commercial lotteries can only be organized by a company with a share capital of at least 1,000,000 euros, and all shares must belong to the Estonian state. This is a state monopoly, and only one company organizes lotteries in Estonia: Eesti Loto AS.

The number of licensed market participants in the gambling sector has been on a continuous upward trend since 2020 (see Table 34).

Table 34. Number of gambling organizer licenses from 2020 to 2024

Year	2020	2021	2022	2023	2024
Number of gambling organizers	20	26	28	34	42

Source: TCB

⁹⁹ According to § 5 (1) of the Gambling Act, remote gambling is the organization of gambling in a manner where the outcome of the game is determined by an electronic device, and the player can participate in the game via electronic communication means, including telephone, Internet, and media services.

Thus, **the number of licensed market participants in Estonia has doubled in four years**, mainly due to the addition of remote gambling service providers whose clientele is international.

Several companies operating in the Estonian market are associated with large international gambling groups that have received fines in various jurisdictions for violating anti-money laundering requirements. One case was identified where an Estonian company was fined.¹⁰⁰ Additionally, companies registered in Estonia have violated the rules established for gambling organizers in Denmark and Sweden.¹⁰¹

The gambling sector has an active umbrella organization – the Estonian Association of Gambling Operators (EHKL), which includes all land-based gambling operators and some remote gambling operators (currently 15 members).¹⁰²

In 2024, the gross gaming revenue (GGR) of the gambling sector was 467 million euros, with the largest portion coming from remote gambling (79%). However, the revenue of the 37 remote gambling operators licensed in Estonia is not equal, as most of the revenue (82% of the GGR¹⁰³ of remote gambling operators) belongs to ten operators.

A significant portion of remote gambling service providers (companies) are registered abroad (41%), and they have no connection to Estonia other than providing the service, including lacking an office in Estonia, making it difficult to supervise them locally. Most foreign companies with an Estonian gambling operator license are from Cyprus (10) and Malta (6).

The proportion of beneficial owners from Estonia among gambling operators is significantly lower compared to foreign beneficial owners. Some beneficial owners are from high-risk jurisdictions in terms of money laundering (Russia, Belarus, Georgia, Uzbekistan).

Supervision of the gambling sector is divided between two authorities – the TCB issues activity and organization licenses under the Gambling Act and supervises accordingly, while the FIU supervises under the MLTFPA and the International Sanctions Act (ISA). When issuing licenses, the TCB does not check for money laundering risks. Therefore, gambling operators currently do not face the same requirements as other obligated entities when entering the market. Additionally, only the TCB can revoke an activity license if a gambling operator has violated anti-money laundering rules. This has not been done so far, as no such violations have been identified.

The level of vulnerability is also increased by the fact that during the review period, the FIU conducted only a sectoral remote control in the gambling sector and no on-site inspections were carried out. Through sectoral remote control, the FIU collected data to identify the risks and vulnerabilities arising from the activities of gambling service providers operating in Estonia, to assess the risks associated with providing gambling services, and to develop measures to mitigate them. Compliance with anti-money laundering requirements was not checked on a company-by-company basis through remote control.

Some companies registered abroad did not cooperate with the FIU and failed to complete the remote control questionnaire by the specified deadline, resulting in five foreign-registered companies being issued a coercive fine order in 2024 for non-compliance with the FIU's precept. Only after paying the coercive fine did the

¹⁰⁰ <https://www.gamblingcommission.gov.uk/news/article/online-gambling-business-tonybet-fined-gbp442-750>

¹⁰¹ <https://www.spillemyndigheden.dk/en/afgoerelse/order-dreambox-games-ou-breach-anti-money-laundering-act> ja <https://www.spelinspektionen.se/globalassets/dokument/ovriga-dokument/beslut/forbud/hitz-gaming-ou-forbud-att-tillhandahalla-spel-2024-07-01.pdf>

¹⁰² <http://www.ehkl.ee/liikmed> (by 28.03.2025).

¹⁰³ Gross Gaming Revenue.

companies comply with the FIU's precept¹⁰⁴. This situation clearly illustrates that it is more challenging for the FIU to contact foreign companies and conduct on-site inspections. Additionally, there is no requirement¹⁰⁵ for a contact person in the sector.

The results of the remote control revealed that **at least five service providers allow clients to make deposits and/or withdrawals in virtual currencies through virtual currency service providers**. The use of virtual currencies significantly increases the risks and vulnerabilities of the service provider, as it may be difficult to identify the origin of the funds used. Allowing deposits and/or withdrawals in virtual currencies among gambling operators is becoming increasingly common worldwide and is used for committing financial crimes. Currently, the use of virtual currencies in the gambling sector is not regulated in Estonia.

Although the TCB checks the background of beneficial owners and board members when issuing an activity license, including submitting a background check request to the FIU, this is challenging for foreign individuals and companies. Additionally, if the company itself does not notify changes in board members or beneficial owners, this information does not reach the TCB, and they cannot verify the individuals. There is also a risk of using front persons and concealing beneficial owners in the case of foreign companies.

On the positive side, market participants conduct thorough background checks on gambling operators' employees, as the service provider must ensure that a person convicted of a crime is not responsible for conducting gambling, making decisions about participation in gambling, or controlling gambling.

According to the Gambling Act, all gambling operators must identify the player before allowing them to play, making it impossible to visit a land-based casino or remote gambling service provider anonymously. Additionally, remote gambling operators may only accept deposits from the player's own bank account and make withdrawals only to the account from which the deposit was previously made.

According to the MLTFPA, gambling operators also have a specific requirement for the application of due diligence measures – they must be applied at least when paying out winnings, making a bet, or both, if the amount given or received by the client is at least 2,000 euros or an equivalent amount in another currency, regardless of whether the financial obligation is fulfilled in a single payment or several related payments within a one-month period.

Although the legal framework is generally sufficient, market participants have raised questions related to the interpretation of payments. The sector also lacks sector-specific guidelines for the application of due diligence measures.

During the assessment period, the FIU organized one sector-specific training for gambling operators (December 21, 2021, with 41 participants) and other training sessions aimed at all obligated entities.

The number of reports submitted by the sector has increased (see Table 35), but this has mainly been due to CTR reports, while the number of suspicion-based reports has decreased. Notably, in the last year, only ten companies (out of 42) have submitted reports, and 97% of the reports have been submitted by three market participants. Reports have been submitted by both Estonian and foreign companies.

¹⁰⁴ All five companies were fined 2,500 euros. The imposed fine can be considered effective as it achieved its purpose, and the companies complied with the FIU's precept.

¹⁰⁵ MLTFPA § 17 (10).

Table 35. Reports submitted by gambling organizers to the FIU from 2020 to 2024

Type of report	2020	2021	2022	2023	2024
UTR	3	4	18	21	10
UAR	19	5	17	5	12
STR	18	48	68	140	74
CTR	78	86	322	338	1261
TFR-2					1
Total	118	143	425	504	1358

Source: FIU

The FIU has stated in its feedback to the sector that the sector submits very few suspicion-based reports, and the quality of the submitted reports is low, although there are some meaningful reports.

Table 36. Number of reports forwarded to law enforcement agencies from 2020 to 2024

	2020	2021	2022	2023	2024
Gambling organizers	13	12	12	8	12

Source: FIU

5.3. Dealers in Precious Metals and Other Traders

The report separately addresses and assesses companies engaged in the purchase or wholesale¹⁰⁶ of precious metals, precious metal products, or precious stones with FIU licenses (hereinafter “dealers in precious metals”) and other traders who are not subject to licensing requirements.

5.3.1. Dealers in precious metals

The level of vulnerability to money laundering for dealers in precious metals is **medium**.

Dealers in precious metals must have an activity license in accordance with § 70 (1) point 6 of the MLTFPA. To obtain an activity license, a dealer in precious metals must meet the conditions specified in § 72 (1) points 1–3 and § 72 (2) of the MLTFPA. The number of activity licenses in the sector has decreased during the assessment period – as of the end of 2020, there were 112 activity licenses, and as of the end of 2024, there were 94 activity licenses for dealers in precious metals in Estonia.

One of the strengths of the sector is that dealers in precious metals must undergo the FIU’s licensing process to operate, which sets a certain standard for entering and operating in the sector and establishes a supervisory mechanism. Considering the structural reorganizations in the FIU’s activities and the addition of resources during the assessment period, the requirements for passing the licensing process necessary to enter the market have significantly increased compared to the past. Although there is no specific law for the sector, all general requirements of the MLTFPA apply to market participants, and the Penal Code also defines

¹⁰⁶ Except for the purchase or wholesale of precious metals and precious metal products used for production, science, and medical needs.

the offense of operating without a license. Among other things, this ensures that dealers in precious metals have established internal procedures for identifying and reporting suspicions of money laundering and have appointed a contact person for the FIU. This is confirmed by the responses to the survey conducted during the preparation of the national risk assessment.

From the perspective of sector vulnerabilities, there is uneven risk awareness between smaller and larger market participants. This is indicated primarily by the number and content of responses to the survey conducted during the preparation of the risk assessment, as well as the low number of reports of suspected money laundering submitted to the FIU by market participants (see table 37).

Table 37. Reports submitted by dealers in precious metals by type from 2020 to 2024

Type of report	2020	2021	2022	2023	2024
UTR		4	29	15	5
UAR	1				4
STR	12	9	7	11	12
ISR			2		
CTR	42	21	35	35	63
Total	55	34	73	61	84

Source: FIU

For precious metal traders, the expectations of the FIU regarding the fulfillment of the reporting obligation are significantly higher in the case of suspicion-based reports.

Table 38. Reports forwarded to law enforcement agencies in the years 2020–2024

	2020	2021	2022	2023	2024
Dealers in precious metals	20		4	2	1

Source: FIU

Additionally, a vulnerability can be identified in the ambiguity regarding the licensing of precious metal traders. Specifically, there are differing interpretations between the supervisory authority and market participants on whether the trading of investment gold and coins with nominal value falls under the activities covered by the current law. Similarly, there is analogous ambiguity for service providers who offer precious metal purchasing services under a pawnbroker's license, without having the necessary license for precious metal purchasing activities. These ambiguities increase the sector's vulnerability and may lead to situations where companies operating in the market may not be aware of the licensing obligation and/or do not comply with the obligations set out in the MLTFPA.

RISK SCENARIOS AND CASES:

- The main risk scenario for precious metal traders is that products made of precious metals are purchased with criminal, suspicious, or unclear origin assets. For example, a client (company) wanted to buy gold. According to the client's explanations, the origin of the assets was sold real estate, confirmed by public data. The market participant identified from public sources that the company's representative was suspected of embezzlement. The person did not deny the embezzlement in public sources and promised to return the assets with the money received from the sold real estate. The market participant suspected that the transactions might be related to concealing the true origin of the assets.
- Another risk scenario is the sale of precious metals to a precious metal trader, where the origin is related to criminal, suspicious, or unclear activities. For example, a person wanted to sell silver jewelry. The market participant identified that the person had previously been convicted of property crimes. Among the jewelry were women's earrings, although the client was a man. The market participant suspected that the items to be sold might not belong to the client, so the transaction was refused.

The FIU has conducted a total of nine remote and on-site inspections¹⁰⁷ in the precious metals trading sector during the assessed period. Deficiencies were identified in companies' documentation (risk assessment, procedural rules), in the application of due diligence measures, and in data retention. During the observed period, the FIU required one company to fix the identified issues¹⁰⁸ and fined two others for non-compliance¹⁰⁹. In the last two years, according to the supervisory authority, the sector's risk level has not been such as to require supervisory actions, which in turn has influenced the sector's risk awareness and vulnerability. Furthermore, since the sector does not have a continuous reporting obligation, the supervisory authority lacks a detailed overview of the number of active service providers in the market and the volume of services.

The FIU has not organized sector-specific training in 2020–2024 but has conducted two training sessions targeting multiple sectors, including precious metals traders.

5.3.2. Traders

The overall level of money laundering vulnerability in the traders' sector is **high** because there is no licensing requirement, which means there is no clear overview of market participants, and because the sector's risk awareness is low – procedures are lacking, and the sector does not submit reports.

According to § 2(1) of the Trade Act, a trader is a person or entity who, in the course of economic or professional activity, offers and sells goods or offers and provides services. Under § 2(1)(5) of the MLTFPA, the law applies to traders if they receive or make cash payments of at least €10,000 or an equivalent amount in another currency, regardless of whether the financial obligation is fulfilled in a single payment or in several related payments within a one-year period.

Since traders conducting cash transactions are not required to hold a license and the reporting threshold for cash transactions (€32,000, MLTFPA § 49(3)) differs from the threshold for becoming an obliged entity (€10,000, MLTFPA § 2(1)(5)), the actual size of the sector and transaction volumes are unknown. According to

¹⁰⁷ Inspections were carried out in 2020 and 2021.

¹⁰⁸ In 2021.

¹⁰⁹ In 2021.

a study¹¹⁰ by Bank of Estonia, 43% of payments in Estonia are made in cash. Therefore, it can be conditionally concluded that the traders' sector is significant in terms of obliged entities.

The greatest vulnerability in the traders' sector is the complete absence of licensing requirements and market entry conditions. Since there is no licensing obligation, the FIU largely lacks knowledge about market participants and also has no possibility to revoke a license as part of supervision – a measure that usually motivates market participants to comply with legal obligations.

As a result, awareness in the traders' sector is low, and internal anti-money laundering measures and controls are inadequate. Traders generally lack the ability to monitor transactions and do not have IT solutions, which, combined with low awareness, results in a very small number of reports (see table below). This is further evidenced by the number of respondents and the content of responses in the risk assessment survey.

Table 39. Reports submitted to the FIU by traders by type in 2020–2024

Type of report	2020	2021	2022	2023	2024
UTR	3	5	37	47	36
UAR			1		
STR		6	1	1	1
ISR		2	29	1	1
CTR	22	51	27	49	21
TFR				1	
Total	25	64	95	99	59

Source: FIU

Most of the reports submitted by traders come from car dealers. The number of reports and the number of reporting entities are very small and do not correspond to the risk level. The FIU's expectations for fulfilling the reporting obligation are significantly higher, especially for suspicion-based reports (particularly for luxury goods traders).

The FIU has not received any reports from luxury goods traders for years, which indicates that insufficient attention is paid to preventing money laundering. Regarding the quality of reports, the FIU has provided feedback to the sector that in several cases, the reason for submitting a suspicion-based report was unclear.

Table 40. Reports forwarded to law enforcement agencies in 2020–2024

	2020	2021	2022	2023	2024
Traders	3	1		1	1
Total	25	64	95	99	59

Source: FIU

During the observed period, the FIU carried out a total of ten on-site inspections¹¹¹ in the traders' sector. The inspections follow a risk-based approach, and in recent years the FIU has allocated most supervisory resources to other sectors with higher risk levels. However, the high vulnerability of the traders' sector indicates a need to strengthen supervision.

¹¹⁰ <https://www.eestipank.ee/press/uuring-eestlased-eelistavad-ostude-eest-tasumisel-vordselt-nii-sularaha-kui-ka-pangakaarti-22122022>

¹¹¹ Inspections were carried out in 2020 and 2021.

RISK SCENARIOS:

- The main risk scenario in the traders' sector is that goods (e.g., **cars, luxury items**) are purchased **with assets of criminal, suspicious, or unclear origin**. The trader accepts the assets and provides the product in return. In such cases, criminally derived assets end up with the trader, while goods unrelated to criminal activity go to the customer.
- Another way traders can be exploited is when, for example, a used car dealer buys a vehicle that may be linked to crime. For instance, an **Estonian used car dealer made a transfer to a foreign company citing vehicle purchase**. The foreign party withdrew the funds in cash immediately after receipt. Similar patterns were observed in the foreign company's other transactions, raising suspicion of money laundering.
- A third risk scenario involves **fraud schemes related to car sales**. Fraudsters may use a real car dealer's online advertisement, copy it, and change the contact details. An unsuspecting customer transfers money to the fraudsters to buy a car that they do not actually possess.

On 30 May 2024, the Council of the European Union adopted a new anti-money laundering rules package¹¹², which sets a €10,000 limit on cash payments starting 10 July 2027. Since a cap will be imposed on cash payments, traders will no longer be considered obliged entities. The exception applies to persons trading in high-value goods¹¹³ and those dealing in precious metals and gemstones, who will remain obliged entities regardless of cash transactions. Thus, only activities with known higher risks will remain (or be added) to the scope of obliged entities, which is expected to lead to more effective supervision.

5.4. Pawnshops

The level of money laundering vulnerability among pawnshops is **medium**.

Providing pawnshop services requires an appropriate license. The FIU is responsible for issuing, amending, and revoking these licenses. As of 31 December 2024, 100 licenses have been issued. The number of pawnshop licenses decreased by 15 (13%) between 2020 and 2024. Discussions within the working group with private sector representatives revealed that the number of active companies is even lower.

Pawnshops do not have a nationwide umbrella organization to coordinate the implementation of anti-money laundering measures or provide unified guidance to the sector.

Although pawnshop services are in demand, the overall size of the sector is small, with a turnover¹¹⁴ of approximately €4.95 million in 2023. This shows that, in terms of financial volume, pawnshop operations are not comparable to other sectors, especially the financial sector. The average pawn amount is €150, indicating that transactions are generally small. Pawnshops have a broad customer base, meaning their services are used by various consumers, including those who need a small amount temporarily. The sector's clientele consists mainly of Estonian residents, which means the customer risk profile is low, as there are few PEP individuals, persons from high-risk jurisdictions, or legal entities with complex structures.

Pawnshops offer a variety of services, mainly short-term loans secured by items. In addition, they engage

¹¹² <https://www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/>

¹¹³ High-value goods include: jewelry, goldsmith, or silversmith products valued over €10,000 or an equivalent amount in another currency; watches and wristwatches valued over €10,000 or an equivalent amount in another currency; motor vehicles priced over €250,000 or an equivalent amount in another currency; aircraft priced over €7,500,000 or an equivalent amount in another currency; watercraft priced over €7,500,000 or an equivalent amount in another currency.

¹¹⁴ Source: Based on 2023 annual reports of companies holding an operating license in the commercial register.

in buying and reselling gold and silver, selling unredeemed items, and consignment sales. Their services are primarily aimed at people in need of quick cash loans, accepting liquid and valuable items as collateral, such as precious metals and electronics. Although pawnshops are not considered financial institutions under the MLTFPA, their services are essentially financial in nature, and pawn agreements are short-term, lasting up to 35 days.

The conclusions of the national risk assessment report are based on a survey conducted in the pawnshop sector and discussions with sector representatives. The analysis also draws on data collected by the FIU, reflecting supervisory activities and identified violations in this sector. Information about the survey was sent to all licensed companies (96 companies¹¹⁵, February 2025¹¹⁶). Only five respondents (5% of companies) provided feedback, meaning the survey results are not representative and generalizations are difficult. At the same time, the very low response rate highlights the lack of contact between the state (including the supervisory authority) and the sector.

The sector's vulnerability is increased by low awareness of money laundering risks and, consequently, insufficient training, which does not ensure continuous awareness of changing risks. Particularly low risk awareness has been observed among smaller companies. Training sessions are rarely organized by pawnshops themselves or by the FIU. For pawnshops, organizing training is expensive. The FIU has not conducted sector-specific training – pawnshops have only had the opportunity to participate in one multi-sector training session (in 2022).

The lack of awareness among pawnshops and their employees about money laundering risks and MLTFPA requirements is a significant factor increasing vulnerability. In addition, pawnshops face difficulties in conducting employee background checks, as these depend mainly on information provided by the individual (employee) themselves.

Table 41. Reports submitted to the FIU by pawnshops by type in 2020–2024¹¹⁷

Main activity	2020	2021	2022	2023	2024
Pawnshops	0	0	0	1	1
CTR					1
STR				1	
UTR					
UAR					
TFR-1					
ISR					

Source: FIU

The sector's low risk awareness and insufficient training are also reflected in the almost non-existent practice of submitting reports. Between 2020 and 2023, pawnshops submitted only one cash transaction report (CTR) exceeding the threshold, and in 2024 only one suspicious transaction report (STR) was received. This indicates a significant gap, as in addition to the lack of training, there are no sector-specific guidelines, including those for identifying suspicious transactions and warning signs.

¹¹⁵ For those pawnshops that had submitted their 2023 annual report to the commercial register.

¹¹⁶ The survey was conducted in February 2025, but data was collected for the period 2020–2024.

¹¹⁷ See explanations of report types in the summary section "Abbreviations."

Table 42. FIU supervisory activities in 2020–2024

Supervision 2020-2024	
Year	2021
Remote inspection by company	3
Number of on-site supervisions	2
Number of on-site inspections where deficiencies in compliance with MLTFPA requirements were identified	2
Deficiencies in risk assessment	2
Deficiencies in procedural rules/internal control regulations	2
Lack of due diligence measures	2
Revocation of license (person voluntarily surrendered the license)	1
Injunction to remedy deficiencies identified during supervision	1
Coercive fine	1

Source: FIU

In 2021, the FIU carried out three remote inspections based on companies and two on-site supervisions. The on-site inspections revealed several deficiencies in pawnshops' compliance with MLTFPA requirements. Identified shortcomings included deficiencies in risk assessments (two cases), procedural rules/internal control regulations (two cases), and the application of due diligence measures (two cases). To address these issues, one injunction was issued, one coercive fine was imposed, and one company's license was revoked (the pawnshop voluntarily surrendered its license). The administrative enforcement measures applied were effective, and the identified deficiencies were remedied.

RISK SCENARIOS:

The **main risk scenario** for pawnshops is when a client attempts to pledge or sell a stolen item to the service provider. Since the ability to verify ownership and origin of the asset used in the transaction is limited, this creates favorable conditions for the disposal of illegally obtained goods. The client takes stolen items to several different pawnshops, receiving a small amount of cash from each. Because **cash transactions are common and the origin of assets is not always sufficiently checked**, the source of stolen goods is difficult to trace. The criminal then uses the cash to buy drugs or finance other illegal activities. If pawnshop employees lack sufficient awareness of money laundering risks and do not report suspicious transactions, such activity may go undetected.

Another finding by the working group is that the sector has only one large pawnshop company with an effectively organized compliance function, while most smaller pawnshops lack such controls. Therefore, there are very few major players in the sector with sufficient resources to train employees and implement necessary IT systems.

5.5. Auditors

The level of money laundering vulnerability among auditors is **below average**.

The work of a sworn auditor focuses on verifying the client's financial statements – therefore, it is essentially not possible to use the services of a sworn auditor for money laundering (it is not relevant in any classic stage of money laundering). Theoretically, a sworn auditor could contribute to a client's failure to comply with MLTFPA requirements if they detect fraud, a suspicious transaction, or client involvement in money laundering but fail to fulfill their obligation to inform the client's management, law enforcement agencies, and the FIU.

The Estonian Auditors' Association is the professional organization for sworn auditors and audit firms operating in Estonia. It was established in 1999 as a public-law legal entity under the law, with members including all sworn auditors holding the professional qualification in Estonia (341 auditors) and all licensed audit firms (115 legal entities). The Association operates on a self-governing principle to organize audit activities in the accounting field in both private and public interests and to protect the professional rights of its members.

The Audit Activities Oversight Board (AJN) is responsible for organizing supervision in the public interest and taking measures to create conditions for the development of audit activities, achieving and safeguarding the quality of sworn auditors' professional work. AJN is an administrative body of five to seven members that performs tasks assigned by law in accordance with public interests. AJN's role includes state supervision (including issuing and revoking licenses and qualifications; organizing exams; quality control; investigations, including those concerning the Auditors' Association; and conducting disciplinary proceedings within the professional organization).

Table 43. Turnover of the auditors' sector in 2020–2024

Period	Turnover from audit services (financial year*)	Number of sworn auditors (as of the end of the financial year)	Number of audit firms ¹¹⁸ (as of the end of the financial year)
2020-2021	€31.6 million	343	129
2021-2022	€34.1 million	351	129
2022-2023	€43.2 million	341	116
2023-2024	€53.5 million	337	116

*The financial year of audit firms runs from July 1 to June 30.

In the context of the MLTFPA, sworn auditors are considered obliged entities when providing audit services. When performing audit services, sworn auditors do not participate in client transactions, nor do they mediate or advise clients on conducting transactions. They only review and verify data on transactions that have already taken place during the audit. According to professional standards for audit activities, the audit process involves checking whether the data of the client's major and significant transactions match what is recorded in the financial statements. Therefore, auditors do not review all transaction data nor perform a full check of transaction details. For this reason, a suspicious transaction or fraud may go undetected by the auditor.

The services provided by sworn auditors themselves do not pose a significant money laundering risk. However, **potential money laundering threats arising from external processes can affect the economic environment in which the auditors' clients operate.**

¹¹⁸ In this document, "audit firm" refers to an auditor's office.

In the context of the MLTFPA, sworn auditors can contribute to compliance primarily by applying due diligence measures during the provision of audit services, including verifying the accuracy of beneficial ownership information and reporting to the FIU any suspicious transactions and cash transactions exceeding €32,000. The main role of a sworn auditor is to act as an expert in identifying, reviewing, and reporting suspicious or unusual schemes in the audited entity's economic transactions.

A positive aspect for auditors is the strong supervisory system. All sworn auditors and audit firms operating in Estonia are mandatory members of the Auditors' Association. Regular oversight of audit activities through the Audit Activities Oversight Board (AJN) is carried out for all audit firms at least once every six years. Quality control occurs every three years if the audit firm has public interest entities among its clients. Supervision also includes checking compliance with MLTFPA requirements. In addition, the FIU monitors auditors' compliance with AML obligations.

Another positive point is that the number of reports submitted by auditors to the FIU regarding cash transactions has grown significantly over the years. However, it is important to note that behind this positive trend lies another issue: approximately 90% of auditors' reports in 2024 were CTRs (cash transaction reports). This means that suspicion-based reports, which provide more detailed information on potential money laundering cases, remain scarce. This indicates the need to enhance auditors' ability and readiness to detect and report suspicious transactions beyond cash flows.

Table 44. Reports submitted to the FIU by auditors by type¹¹⁹ in 2020–2024

Main activity	2020	2021	2022	2023	2024
Auditors	71	68	63	114	120
CTR	62	57	46	94	108
STR	5	6	7	9	3
UTR	1	2	2	5	5
UAR	2	3	5	5	1
ISR			3	1	3
TFR-1	1				

Source: FIU

The reports submitted by the sector have been extremely important. The information obtained from them was forwarded to Estonian investigative authorities, demonstrating their direct value in the fight against crime.

Table 45. FIU reports to Estonian law enforcement agencies in 2020–2024

	Reports submitted to law enforcement agencies 2020–2024				
	2020	2021	2022	2023	2024
Auditors	28	1	1	3	2

Source: FIU

¹¹⁹ See explanations of report types in the „Abbreviations“.

The vulnerability of the sworn auditors' sector can be attributed to the opacity of clients' transactions, which makes it difficult for auditors to assess the actual economic substance and identify potential risks. The sector is further weakened by auditors' insufficient cooperation with other obliged entities (such as credit institutions, insurers, or virtual asset service providers), which hinders the detection of suspicious transactions. Inadequate legislation, which does not require obliged entities to share information with auditors, exacerbates the problem.

This means that Estonian law lacks a clear provision obliging audited companies to provide auditors with all necessary data during the audit. The FIU's insufficient feedback to auditors regarding the fulfillment of the reporting obligation for suspicious transactions and the use of the information received reduces auditors' motivation and effectiveness in detecting and reporting suspicious transactions, as the impact and usefulness of such reports remain unclear. This, in turn, increases vulnerability to money laundering, as auditors' contribution to preventing money laundering is essential for ensuring transparency in the financial system.

It is worth noting that Estonia lacks specific money laundering typologies and guidelines (including indicators) tailored to the auditors' field of activity for recognizing suspicious transactions and activities, i.e., warning signs. This gap may limit auditors' ability to identify and understand money laundering risks associated with their clients' financial transactions. There have also been deficiencies in the quality of suspicious transaction reports, which may, in turn, reduce the effectiveness of reports and the supervisory authorities' ability to prevent money laundering.

Table 46. Formal quality of reports

	2022		2023		2024	
	Number of reports	problematic % ¹²⁰	Number of reports	problematic %	Number of reports	problematic %
Auditors	2	12%	3	15%	6	50%
Missing additional documents	1	6%			1	8%
Content errors (Transaction description incomplete, content unclear)	1	6%	1	5%		
Formatting errors (e.g., persons not indicated)			2	10%	5	42%

Source: FIU

Therefore, it is important to organize targeted training on money laundering typologies to increase auditors' awareness and ability to identify money laundering risks. In addition, it is essential to make market participants aware of the list of higher-risk countries and the principles behind its compilation to help them better assess client risks and apply appropriate due diligence measures.

The efficiency and quality of auditors' work is significantly hindered by limited access to essential independent and reliable databases, particularly the Land Register and the Criminal Records Database. Access to the Land Register and the Criminal Records Database is subject to a fee, and for access to another individual's

¹²⁰ When calculating the share, CTR reports were excluded from the total number of reports, as they are primarily analyzed by machine.

data in the latter, a legal basis or legitimate purpose is required. Such access restrictions prevent auditors from conducting thorough risk assessments, which are crucial during an audit.

Auditing companies engaged in virtual assets is often a challenge for auditors, and auditors tend to refuse such clients because these companies generally have a low level of accounting organization and incomplete accounting data. In addition, virtual asset service providers often fail to apply proper due diligence measures, which increases vulnerability. This situation highlights the need to improve the quality of accounting and due diligence measures in companies operating in the virtual asset sector and to raise auditors' awareness of the risks in this field.

As part of the risk assessment, a survey was conducted in the sector. An invitation to participate in the survey was sent to all 115 audit firms¹²¹, and responses were received from 47 audit firms (40% of all audit firms). The survey results indicate as a strength that all respondents are aware of AML requirements, have mechanisms for independence and due diligence, including client risk assessment, and have established procedures for implementing FIU notifications. Regular training for employees, including internal training, is provided. A weakness identified is that some audit firms lack technical solutions for risk management, which is mainly a problem for smaller audit firms employing 1–5 sworn auditors. A barrier highlighted was the absence of a database for identifying politically exposed persons and foreign beneficial owners. Up to 10% of clients are e-residents, and deficiencies or unavailability of remote identification systems may pose significant vulnerability. It is difficult to assess risks and verify data related to foreign clients. Audit firms include both network firms and sole practitioners, and access to technical solutions and foreign databases is mainly limited for smaller audit firms.

Table 47. FIU supervisory activities in 2020–2024

ML/TF inspections carried out by the FIU	
Year	2020
Remote inspection based on company	10
Number of remote inspections where a deficiency in compliance with AML requirements was identified	2
Number of on-site inspections	5
Number of on-site inspections where a deficiency in compliance with AML requirements was identified	2
Deficiencies in procedural rules/internal control regulations	2
Deficiencies in reporting obligations	2
Order to eliminate deficiencies identified during supervision	2

Source: FIU

The FIU conducted supervisory proceedings only in 2020, and the main reason for the limited supervision is a lack of resources. Orders to remedy deficiencies were issued with the aim that the auditor would eliminate the shortcomings identified during the supervisory process in procedural rules/internal control regulations. The orders to remedy deficiencies were fulfilled, which demonstrates that the supervisory authority's actions have concrete consequences and enforcement measures are effective.

¹²¹ The number of audit firms, 116, is presented in the table as of the end of the financial year (30.06.2024). The survey was sent to audit firms holding an operating license at the time of the survey – between the financial year-end date and the date the questionnaire was sent, some audit firms exited and new ones joined (license expiration/acquisition), hence the difference in numbers.

Table 48. FIU supervisory activities in 2020–2024

Misdemeanor proceedings 2020–2024					
Person under proceedings	Natural person / Legal person	Year	ParagraPH	Procedure type	Penalty
Audit firm	Natural	2020	MLTFPA § 92 (1)	Expedited procedure	Fine
Audit firm	Natural	2020	MLTFPA § 92 (1)	Expedited procedure	Fine

Source: FIU

In 2020, the FIU identified two cases during supervisory proceedings where an auditor had failed to notify the FIU of a client’s large cash transaction in the manner prescribed by law. Such conduct constitutes a clear violation of MLTFPA requirements and underscores the need to strengthen supervision and ensure compliance with the law. Misdemeanor proceedings were initiated regarding the identified deficiencies, and two auditors were fined. Problems persisted in identifying foreign politically exposed persons and beneficial owners, particularly in situations where relevant registers or data were lacking in the foreign jurisdiction.

RISK SCENARIOS:

Risk typologies include risks of unusual economic activity, where the client’s operations or transactions are economically unjustified or differ significantly from the usual business model, involving suspicious cash transactions and disproportionate profitability. Also, risks related to concealment of identity and lack of transparency, where the client aims to hide their true identity, beneficial owners, or the origin of funds by using, for example, front persons, complex legal structures, or jurisdictions that allow anonymity.

To enhance auditors’ compliance with MLTFPA requirements, it is important for the Estonian Auditors’ Association and the FIU to communicate clear messages and observations to market participants. Auditors can also benefit from the Auditors’ Association’s guidance document “Sample Procedural Rules for Compliance with Anti-Money Laundering and Counter-Terrorist Financing Obligations” (last updated on 22.12.2022), which includes updated procedural rules, changes compared to the 2018 rules, and Annex 1 to the procedural rules, which addresses client acceptance and contains the client-specific risk assessment model required by the MLTFPA. FIU guidelines, which are very important, can be found on the FIU’s website¹²².

¹²² <https://fiu.ee/oigusaktid-ja-juhendid/juhendid>

Table 49. Trainings conducted in the auditors' sector during the assessment period

Date	Theme	Training session host
17.06.2020	Board of Auditors Members' Information Day	the Board of Auditors
21.12.2020	Best Practice Day 2020	the Board of Auditors
21.10.2021	Board of Auditors Autumn Information Day 2021	the Board of Auditors
22.11.2021	Crypto – What Should an Auditor Know?	the Board of Auditors
25.01.2022	Tax and Legal Conference 2022	the Board of Auditors
14.10.2022	Training on the Assessment of Own Funds for VASPs	FIU, the Board of Auditors
30.05.2023	Board of Auditors Spring Information Day 2023	the Board of Auditors
08.06.2023	AML	FIU
10.10.2023	Auditors' Roundtable: Audit/Review and Own Funds Control of Virtual Currency Service Providers	the Board of Auditors
31.10.2023	Board of Auditors Autumn Information Day 2023 and FIU Feedback and Expectations for Auditors	FIU, the Board of Auditors

Source: FIU

To ensure auditors' continuous awareness and up-to-date skills, the Estonian Auditors' Association regularly publishes a monthly newsletter for sworn auditors and audit firms, which can be read on the Association's website¹²³. In addition, among other training programs, the Association organizes supplementary courses on anti-money laundering. Participation in these trainings is mandatory for auditors to the extent prescribed by law.

5.6. Other Providers of Legal Services

The level of money laundering vulnerability for other legal service providers is **medium**.

Other legal service providers are subject to the MLTFPA in the course of their economic, professional, or official activities. Lawyers who are not members of the Estonian Bar Association but provide legal services are obliged to comply with anti-money laundering rules under § 2(2) of the MLTFPA.

In Estonia, providing legal services as a lawyer is not regulated or restricted, except when the lawyer is a member of the Estonian Bar Association and operates under the professional title of attorney. In such cases, the Estonian Bar Association exercises professional supervision over the attorney. This section addresses only lawyers who are other legal service providers, i.e., not members of the Estonian Bar Association. The vulnerability of the lawyers' sector is described in subsection 5.11.

The umbrella organization for legal service providers is the Estonian Lawyers' Union, which is a voluntary association and does not have regulatory or supervisory functions. The obligation to supervise compliance with the MLTFPA requirements lies with the FIU. It is an open market where the provision of services listed in the MLTFPA is at the discretion of each service provider, and where the implementation of the MLTFPA often falls under the responsibility of other legal service providers. Market entry is not regulated, and service providers do not need registration or a license.

¹²³ <https://www.audiitorkogu.ee/est/uudiskirjad>

The Estonian Lawyers' Union has not yet implemented measures to ensure anti-money laundering compliance by other legal service providers nor issued guidelines for the sector. Nevertheless, the Union is a respected organization whose positions and guidance are taken into account in the field, meaning it could influence market participants to some extent.

As of 07.01.2025, the Estonian Lawyers' Union had 480 members. In addition to members of the Bar Association and the Lawyers' Union, legal services in Estonia are also provided by other consultants, whose exact number is unknown. In practice, it is very difficult to distinguish legal service providers because the state lacks an appropriate control mechanism over the sector. Other legal service providers who have indicated in the Business Register their economic and professional activity code (EMTAK) as 69102 "activities of legal consultants and law offices" numbered between 770 and 841 companies during 2020–2023, with annual turnover ranging from €18 million to €22.7 million.

Clients of other legal service providers are mostly local—individuals or small and medium-sized enterprises. The umbrella organization has no supervisory function. Oversight of the sector is carried out by the FIU, for whom compiling a risk analysis related to the activities of other legal service providers is challenging. There is a lack of sufficient initial data for more detailed analysis, as well as knowledge of whether other legal service providers have been penalized under criminal or misdemeanor proceedings for violations of the MLTFPA.

Legal service providers are important gatekeepers in preventing money laundering due to their access to the financial system and legal structures, client trust, professional expertise, and role in facilitating significant transactions. They are obliged to know their clients and their transactions and to report suspicious activity. Effective compliance with due diligence obligations makes them a key barrier to illicit money flows, but their position and knowledge can also be misused.

The conclusions presented in the report are based on a survey conducted among other legal service providers as part of the national risk assessment and discussions with sector representatives. Information about participation in the survey was sent to all companies operating under the EMTAK code for legal consultants and law offices (929 companies¹²⁴, February 2025). Feedback was provided by 112 individuals, representing 12% of companies, and based on responses, 26% of legal service providers have offered services listed in MLTFPA. However, turnover from services provided as obliged entities cannot be separated from other services, as such accounting does not exist. Specifically, seven respondents identified themselves as providers of services described in MLTFPA, representing less than 3% of known service providers, meaning the survey results carry little weight and it is difficult to generalize for the entire sector. Nevertheless, the results reflect certain aspects of the sector, such as the fact that the state lacks contact with the sector as a whole.

On the negative side, market participants in the sector are currently undefined, making it difficult to reach them for AML/CFT guidance or supervision. Most survey respondents had risk management system documents related to MLTFPA in place or under development. However, this is not confirmed by the small number of reports submitted to the FIU over the past five years (an average of only five reports per year from the entire sector across all types of reports), indicating that actual risk awareness in the sector is low and risks are not sufficiently identified. Reasons may include the absence of entry controls (anyone can offer services) and uncertainty about who exactly provides services as obliged entities under MLTFPA. None of the reports submitted to the FIU by other legal service providers were forwarded to investigative authorities. Nor was a separate analysis conducted on reports submitted by this specific sector to the FIU to assess their quality.

¹²⁴ Business Register data as of 2024.

Table 50. FIU reports to Estonian law enforcement agencies in 2020–2024¹²⁵

Main activity	2020	2021	2022	2023	2024
Other legal services	1	12	3	5	4
CTR		1			
STR		4	1	4	1
UTR	1	1			
UAR		6	1		1
ISR			1	1	2

Source: FIU

The few reports received by the FIU indicate that market participants' awareness of money laundering risks needs improvement. It should be noted, in particular, that the FIU has not yet organized sector-specific anti-money laundering training.

To enhance risk awareness in the sector, **it is important that other legal service providers participate more actively in FIU information sessions and general training. This would help them better understand the risks associated with their activities and, in turn, more effectively identify suspicious situations in their business operations, thereby avoiding involvement in money laundering schemes.** Submitting reports on suspicious transactions, in turn, enables the FIU to collect pieces of information from different sectors to piece together larger money laundering schemes, where every detail can be crucial for detecting a crime.

Although Estonia has established anti-money laundering legislation, there is no effective supervisory system among legal service providers, and during 2020–2024 the FIU did not initiate supervisory proceedings or prepare sector-specific guidelines for other legal service providers. Therefore, there is a risk that money laundering risks are underestimated in the sector.

All survey respondents assessed that the share of e-residents in their client base is less than 5%. E-residents are not considered different from other clients in terms of risk level or treatment. All respondents also indicated that, in addition to e-residents, they provide services to non-residents to a greater or lesser extent. However, it is not possible to conclude what proportion of the total number of clients non-residents represent in the sector. It can be noted, however, that more than half of the respondents do not provide services to persons from high-risk third countries. Of those respondents who do provide services to persons from high-risk third countries (3 respondents), they estimate the share of such clients to be between 1–19%.

Risks associated with the activities of other legal service providers fall into different typologies. First, there is the risk of insufficient knowledge and compliance with regulations, which arises when the service provider lacks adequate understanding of applicable requirements and legal norms (e.g., MLTFPA). This ignorance risk may lead to situations where the service provider unknowingly supports illegal activities. Second, there is the risk of opacity and conflict of interest, where the legal service provider is involved in the management of companies whose actual activities are unclear. This also includes the risk that the legal service provider is exploited, for example, in the creation of anonymous companies whose subsequent activities remain unknown.

¹²⁵ See explanations of report types in the „Abbreviations“.

Third, there is a money laundering risk arising from the service provider's inability to verify the origin of funds used to pay for the service or from underestimating the associated risks, thereby opening the door to illicit money flows.

Fourth, there is also a risk of abuse of legal structures, which is linked to services related to the establishment, reorganization, and liquidation of companies. Such structures can be used to conceal the identity of beneficial owners and integrate illicit proceeds into the country's economic system.

On the positive side, other legal service providers have an umbrella organization—the Estonian Lawyers' Union—which promotes and values the legal profession and offers sector participants opportunities to share knowledge and experience. Although the full size of the sector is unknown, the total turnover of companies operating under the legal consultancy and law office activity code is small compared to other sectors, and based on survey results, other legal service providers minimally offer services as obliged entities.

5.7. Bailiffs and Bankruptcy Trustees

The level of money laundering vulnerability for bailiffs (hereinafter "bailiffs") and bankruptcy trustees (hereinafter "trustees") is **below average**.

In the national risk assessment, the vulnerability of bailiffs and trustees was addressed jointly. Although their official or professional activities generally differ from each other, bailiffs and trustees are considered obliged entities under MLTFPA for the same types of transactions. Therefore, the working group concluded that the vulnerability of both sectors can be assessed together.

Bailiffs and trustees are obliged entities only when providing the services listed¹²⁶ in § 2(2)(1–5) of MLTFPA. In practice, since bailiffs and trustees are obliged entities only when offering certain services, they mainly encounter money laundering risks in real estate auctions. Consequently, their vulnerabilities were assessed primarily in connection with services related to real estate auctions.

The Chamber of Bailiffs and Bankruptcy Trustees (hereinafter "KPKoda") is a public-law legal entity established by law, which develops anti-money laundering guidelines for the sectors and trains its members on money laundering risks. In addition to guidelines, KPKoda prepares opinions, explanations, and informational materials for its members. Between 2020 and 2024, KPKoda prepared guidelines for compliance with MLTFPA requirements.

As of 31.03.2025, there are 38 bailiffs and 58 trustees in Estonia (30 of whom are sworn advocates). It is important to note that sworn advocates receive additional training on areas related to MLTFPA from the Estonian Bar Association, which significantly improves their awareness and expertise, contributing to the fight against money laundering.

¹²⁶ Bailiffs and bankruptcy trustees are obliged persons under § 2(2) of the MLTFPA both in their professional and official activities. This includes financial or real estate transactions, transaction guidance, and official acts/services related to: (i) the purchase/sale of real estate, a business, or shares in a company; (ii) managing a client's assets; (iii) opening/managing payment, deposit, or securities accounts; (iv) obtaining funds necessary for establishing, operating, or managing a company; (v) establishing, operating, or managing trusts, companies, foundations, or other associations without legal personality.

Table 51. Number of bailiffs and bankruptcy trustees in 2020–2024

Year	Bailiffs	Bankruptcy trustees (of which sworn advocates)
2024	39	61 (31)
2023	38	61 (29)
2022	39	65 (28)
2021	39	69 (30)
2020	40	73 (32)

Source: KPKoda

The number of bailiffs and trustees has remained stable. At the time of preparing this report, a reform was initiated to transfer the enforcement of public-law claims from bailiffs to the TCB. This would significantly reduce the workload of some bailiffs and their ability to maintain their offices. If the reform is implemented, only 15–20 bailiffs would remain in office.

To start professional activity, both bailiffs and trustees must pass a qualification exam, which also assesses their knowledge in the field of anti-money laundering. Bailiffs are appointed indefinitely by the Minister of Justice. They operate through self-financing offices and must undergo continuing education checks or take an exam every five years. Bailiffs are appointed through a competitive process; those who pass the exam may work as assistants. The last new bailiff was appointed in 2015. Trustees can qualify based on the Chamber's exam or, exceptionally, through the Professional Council as sworn advocates, sworn auditors, or bailiffs. Trustees are appointed by the court, which also assigns them to bankruptcy proceedings. A trustee's task is to conduct bankruptcy proceedings in accordance with the Bankruptcy Act. There is no time limit for acting as a trustee, but continuous professional development and a five-yearly continuing education check are required; if continuing education is not properly completed, the trustee is directed to retake the exam.

Both bailiffs' and trustees' activities are regulated by a state mandate granted by either the court or the Ministry of Justice. Their work is based on special laws such as the Code of Enforcement Procedure (TMS) and the Bankruptcy Act (PankrS). In addition to these laws, the MLTFPA plays an important role in preventing money laundering.

According to the survey, clients of bailiffs and trustees include e-residents, politically exposed persons (PEPs), legal entities with complex structures, and clients from high-risk jurisdictions, all accounting for less than 5%. Bailiffs handle an average of 100–1,400 cases per year, with most clients being professional creditors such as banks and state institutions, while debtors are mainly Estonian residents. Overall, the services of trustees and bailiffs are not considered particularly attractive to criminals or money launderers.

The conclusions presented in this report are based on a survey conducted among bailiffs and trustees as part of the risk assessment and discussions with sector representatives. The analysis also draws on data collected by the FIU, reflecting supervisory activities and identified violations in this sector. The survey examined perceptions of administrative coercion and sanctions, staff preparation and competence, applied due diligence measures, compliance with reporting obligations, and client awareness and identification. A total of only 22 individuals responded (22%): 9 bailiffs and 13 trustees.

According to court statistics for 2023 and 2024, the number of insolvency petitions filed by individuals was 1,114 and 1,091 respectively; bankruptcy petitions filed by legal entities were 248 and 296; and petitions filed by creditors were 215 and 323—making a total of 1,577 and 1,710 respectively.

According to bankruptcy decision statistics, in 2023 a total of 131 bankruptcies of natural persons and 140 bankruptcies of legal entities were declared, and in 2024 69 bankruptcies of natural persons and 151 bankruptcies of legal entities were declared. Bankruptcy proceedings were terminated due to abatement for 240 persons in 2023 and for 314 persons in 2024 (including both natural and legal persons). On other statutory grounds, bankruptcy proceedings were terminated for 151 persons in 2023 and for 238 persons in 2024 (including both natural and legal persons).

Table 52. Bankruptcy decision statistics for 2020–2024

Year	2020	2021	2022	2023	2024
Natural persons					
Bankruptcy declaration	635	555	363	131	69
Termination of bankruptcy proceedings (§ 29(1) and § 158)	119	126	131	131	188
Termination based on other legal grounds	81	65	48	43	50
Legal entities					
Bankruptcy declaration	150	103	100	140	151
Termination of bankruptcy proceedings (§ 29(1) and § 158)	188	160	115	109	126
Termination based on other legal grounds	80	104	86	108	188

Source: MoJD

Although the statistics do not include information on the size of the bankruptcy estate, it can be stated that since most bankruptcy proceedings are discontinued due to lack of funds—meaning the debtor has no resources to finance the process and the proceedings are assetless—the risk level for transactions sanctioned or prohibited under the MLTFPA during bankruptcy proceedings is rather low. Therefore, the inherent vulnerability of bankruptcy proceedings to money laundering is also relatively low.

Between 2020 and 2024, the number of real estate auctions in the auction environment has fluctuated between 2,384 and 3,782. The number of auctions that resulted in a sale during the same period ranged from 693 to 905. In 2021, sales were exceptionally strong, whereas in 2024 the number of auctions was the highest, but the number of completed sales was the lowest.

Table 53. Real estate auctions in the auction environment in 2020–2024

Year	Number of Auctions	Ended in Sale	Total Sales Price (EUR)
2020	3,782	772	33,549,216
2021	3,026	905	110,549,335
2022	2,384	712	45,122,397
2023	3,203	714	40,505,100
2024	3,628	693	37,526,372

Source: KPKoda

The overall volume of the bailiffs' and trustees' sector is relatively modest (the sector's total turnover is €40,505,099¹²⁷) and their client base consists mainly of low-risk individuals. In addition, the share of cash transactions in the sector is small, which reduces the direct risk of money laundering. Nevertheless, it should be emphasized that despite the small overall volume and low-risk client base, trustees and bailiffs may still be involved in money laundering schemes, and the sector can be used to facilitate (tax) fraud.

A potential money laundering scheme could involve creating an enforcement document artificially (e.g., a payment order in expedited proceedings or a notarized acknowledgment of debt) and submitting it for enforcement to a bailiff. Since a bailiff does not have to verify the origin of the assets when seizing property based on an enforcement document, the risk of money laundering in such a scenario cannot be ruled out. Another scenario is acquiring property at auction using cash. Therefore, it is extremely important to implement additional measures to prevent and detect possible abuses.

Table 54. Statistics on supervisory proceedings by the FIU

Supervisory proceedings 2020-2024		
Sector	Bailiffs	Bankruptcy trustees
Year	2020	2021
Company-based remote inspection	10	7
Number of remote inspections identifying deficiencies in MLTFPA compliance	1	1
Number of on-site supervisions		2
Number of on-site inspections identifying deficiencies in MLTFPA compliance		2
Deficiencies in procedural rules/internal control regulations	1	3
Injunction to rectify deficiencies identified in supervision	1	2

Source: FIU

The FIU supervised bailiffs and trustees only in 2020–2021, mainly through remote inspections. On-site inspections of trustees in 2021 revealed more violations of the MLTFPA than remote inspections, indicating the effectiveness of on-site supervision. Orders to remedy deficiencies were issued with the aim that the bailiff/trustee corrects the shortcomings identified during the supervisory procedure in procedural rules/internal control regulations. These orders were complied with, demonstrating that the supervisory authority's actions have tangible results and enforcement measures are effective.

The limited resources of the supervisory authority have led to insufficient supervision in recent years. FIU has focused on higher-risk sectors, but strong supervision, especially through on-site inspections, is necessary in this field.

It is important to strengthen the risk-based approach and improve staff training. Shortcomings are also caused by the fact that training organized by the supervisory authority is scarce, and participation by market participants in other anti-money laundering training is limited due to high costs. During the observed period, the FIU did not organize sector-specific training; only one joint training session was held for several sectors at once, which is insufficient to ensure awareness of money laundering risks and compliance with MLTFPA requirements.

¹²⁷ Total final prices of real estate sold at auctions organized by bailiffs and bankruptcy trustees.

Table 55. Reports submitted to FIU by the sector in 2020–2024¹²⁸

Main activity	2020	2021	2022	2023	2024
Bailiffs	0	1	1	2	1
STR		1		1	1
UTR				1	
ISR			1		
Bankruptcy trustees	0	2	2		2
STR		1	2		1
UTR		1			
UAR					1

Source: FIU

Bailiffs submitted only five reports to the FIU during the period 2020–2024. In 2020, no reports were received from them. The highest number of reports (2) was submitted in 2023, and in 2024 one report was submitted. Trustees submitted slightly more reports (6) during the same period. In both 2020 and 2023, trustees did not submit any reports. Although the overall number of reports was low, trustees submitted two reports in both 2021 and 2022, which represented the highest number of reports during those years.

Table 56. Reports submitted by the FIU to law enforcement agencies in 2020–2024

	Reports submitted to law enforcement agencies 2020–2024				
	2020	2021	2022	2023	2024
Bailiffs				1	

Source: FIU

The few reports submitted by the sector were extremely important. In 2023, the sector submitted only two reports, but the information obtained from them has been highly significant and has led to referrals to Estonian investigative authorities. This demonstrates the direct value of such reports in the fight against crime. Therefore, strengthening the capacity of the bailiffs and trustees sector to identify suspicious client activities and/or transactions is a crucial step in combating money laundering. Several factors lie behind the low level of reporting activity. While the limited training offered by the FIU and the Chamber of Bailiffs and Trustees may be one reason, it is also important to consider insufficient supervision and the lack of sector-specific guidelines (including concrete indicators of suspicious transactions). Improving transaction monitoring, promoting cooperation with the supervisory authority, and strengthening internal control procedures are also essential. Monitoring of suspicious transactions is mainly carried out manually, due to both a lack of awareness and limited financial resources for investment.

Deficiencies in data quality, timeliness, and availability hinder the application of due diligence measures by bailiffs and trustees. Although client data is collected through KYC questionnaires, verifying TEKSA data is difficult, and there is no systematic control over its timeliness. There are also challenges in identifying politically exposed persons (PEPs), especially foreign individuals, due to the lack of access to foreign databases containing information on foreign PEPs.

¹²⁸ See explanations of report types in the „Abbreviations“.

On the positive side, the activities of bailiffs and trustees focus primarily on the sale of debtors' assets, which means there are fewer risks and opportunities for money laundering compared to operating companies (such as complex transaction structures, continuous cash flow, international partners, diverse client relationships, and a wide range of services or products). Bailiffs and trustees are also required to collect data on transaction parties together with credit institutions and notaries, and this additional control makes their services less attractive to criminals.

5.8. Accountants and Tax Advisors

The level of money laundering vulnerability for accountants and tax advisors is **medium**.

The Estonian accounting and tax advisory services sector is diverse, encompassing both small businesses and larger accounting firms. Their clientele ranges from individual entrepreneurs to international groups, making the sector structurally varied and vulnerable. The main services provided include preparation of accounting documents and transaction recording, tax accounting, reporting, tax consulting, and business support services. A key characteristic of Estonian accounting and tax advisory companies is the absence of direct professional regulation: certification is voluntary, no operating license is required, and there is no statutory supervision of the sector or obligation to belong to a professional association. Essentially, anyone can establish an accounting or tax advisory company, and service conditions are agreed upon with the client.

Under § 2(1)(7) of the MLTFPA, providers of accounting services are required to comply with the law. The same obligation applies under § 2(1)(8) of MLTFPA to companies providing accounting and tax advisory services. The Accounting Act, tax laws, and other acts set obligations for companies (board responsibility) regarding accounting and tax reporting, but companies can decide how to organize their accounting.

Accountants and accounting firms are represented by the professional association Estonian Association of Accountants (ERK), which has been the certifying body for accountants since 2004 and has issued over 5,200 certificates. ERK has also established a committee for accounting service providers to address topics relevant to accounting firms and issues a recognized quality label for accounting companies (21 labels issued in total). ERK is a voluntary association and does not have regulatory or supervisory functions. The FIU is responsible for supervising compliance with MLTFPA requirements.

As of 31 December 2024, ERK had approximately 620 members, including 162 legal entities (126 accounting firms). Other companies providing accounting and tax advisory services that are not ERK members numbered 8,687 (EMTAK 69202). Since it is not possible to distinguish whether this is the main or secondary activity, an estimate based on the statistics of the information portal teatmik.ee¹²⁹ indicates that about 80% (7,474 companies) have accounting services as their main activity.

According to teatmik.ee, the overall market volume for accounting services (EMTAK 69202 as the main activity) was approximately €219 million. The largest companies accounted for about 70% of the market volume. Most companies had a small turnover: in 2024, only 320 companies (approximately 3.63% of the sector) exceeded a turnover of €100,000. At the same time, the combined turnover of the 380 largest accounting companies during the four quarters of 2024 amounted to €162,347,000.

¹²⁹ <http://www.teatmik.ee/et>

Table 57. Sector turnover statistics, overview of the 380 largest companies in the accounting field

Activity	EMTAK	Number of companies	Aggregate turnover of the last 4 quarters
Accounting, Tax Advisory	69202	366	146,757,000
Bookkeeping, Accounting, and Auditing; Tax Advisory	6920	11	1,782,000
Auditing	69201	2	13,381,000
Business Consulting and Other Management Consulting	70221	1	427,000
Total		380	162,347,000

Source: Äripäeva Infopank

The conclusions presented in this report are based on a survey conducted among providers of accounting and tax advisory services as part of the risk assessment, as well as discussions with sector representatives. In addition, the analysis is based on data collected by the FIU, reflecting supervisory activities and identified violations in this sector. Information for participation in the survey was sent to companies providing accounting and tax advisory services under EMTAK code 69202 (851 companies, December 2024). A total of 125 responses were received, representing 14.7% of the companies contacted, which accounts for 1.4% of known service providers (125/8,813¹³⁰).

Negative aspects: The accounting and tax advisory sector is characterized by a non-existent entry barrier, allowing virtually anyone to operate in the field, bringing service providers with varying levels of competence and awareness to the market. Unlike large international firms with effective internal control mechanisms and high awareness of anti-money laundering (AML) requirements, the majority of service providers are small businesses where such mechanisms are either basic or absent. Consequently, the sector's vulnerability is primarily reflected among micro and small enterprises, which often lack expertise, technical capacity, financial resources, and motivation to comply with AML requirements.

The size of an accounting or tax advisory company's turnover does not determine the size or sector of the clients served. However, the size of the service provider does influence its awareness of AML requirements and its technical capacity to operate in this area. The FIU has identified low quality in companies' risk assessments and internal procedures during supervisory processes, indicating deficiencies in internal control mechanisms and insufficient effectiveness of measures in detecting and mitigating actual money laundering risks.

Additional challenges: There is a lack of adequate IT solutions for identifying politically exposed persons (PEPs) and foreign beneficial owners. Smaller service providers have limited access to paid databases due to high costs. Furthermore, service providers do not pay sufficient attention to clients and transactions originating from or linked to high-risk countries, which increases the level of money laundering risk.

The working group has identified that the sector makes limited use of agents, i.e., larger firms mediating clients to smaller service providers. The use of agents can lead to insufficient application of due diligence measures and help conceal actual cash flows, thereby creating a favorable environment for money laundering, especially since there is no clear overview of the ultimate clients' activities and background.

The survey revealed that although 40% of accountants have no e-resident clients and most (37% of respondents) have a share below 10%, this is not a direct indicator of increased vulnerability across the entire sector. Vulnerability stems rather from the sector's unregulated nature, insufficient supervision, and the lack

¹³⁰ A total of 8,813 company contacts were identified under EMTAK code 69202 (accounting services).

of awareness and resources among small businesses to comply with AML requirements. Risks related to e-residents are likely concentrated among a smaller group of service providers with a larger e-resident client base, and these require further analysis considering general indicators of money laundering suspicion (e.g., complex identification, use of proxies).

Although Estonia has AML legislation in place, there is no effective supervisory system among accounting and tax advisory service providers, and during 2020–2024 the FIU has not conducted supervisory procedures (including remote and on-site inspections) nor prepared special guidelines for accounting and tax advisory service providers. This creates a risk that money laundering risks in the sector are underestimated.

Reporting activity by accounting and tax advisory service providers is low. During 2020–2024, only a very small percentage of the entire sector submitted reports to the FIU. The highest share was in 2024, reaching 0.37% of all obliged entities in the sector. Although the percentage is small, an increase in reporting activity can be observed: significantly more reports were submitted in 2024 than in previous years. The working group found that the reporting obligation is mainly fulfilled by larger service providers. Low reporting activity indicates sector vulnerability, as potentially suspicious client activities and/or transactions are likely to remain undetected and unreported. Although Table 58 shows the number and types of reports by year, the submitted reports have not led to further investigations, prosecutions, or convictions by law enforcement authorities, indicating issues with their quality and subsequent usability. Additionally, it should be noted that the supervisory authority has not developed special guidelines or specific indicators for recognizing suspicious transactions or warning signs for the sector.

Table 58. Reports submitted by accountants to the FIU by type¹³¹ during 2020–2024

Main activity	2020	2021	2022	2023	2024
Accountants and tax advisors	21	14	21	24	34
CTR	14	5	10	13	9
STR	1	5	4	2	7
UTR	4	1	3	1	8
UAR	2	3	4	5	8
TFR-1					1

Source: FIU

The few reports submitted by the sector are nevertheless very important. The information obtained from them is significant and has been forwarded to Estonian investigative authorities, demonstrating the direct value of such reports in the fight against crime. Therefore, strengthening the capacity of the accounting and tax advisory sector to identify suspicious client activities and/or transactions is an extremely important step in combating money laundering.

¹³¹ See explanations of report types in the „Abbreviations“.

Table 59. Reports submitted by the FIU to Estonian law enforcement agencies during 2020–2024

	Reports submitted to Estonian law enforcement agencies 2020–2024				
	2020	2021	2022	2023	2024
Accountants and tax advisors	3				2

Source: FIU

The FIU has attempted to improve sector awareness through various training sessions. However, the number of participants has been significantly low, considering the large number of service providers operating in the sector. Despite the FIU's efforts, awareness of anti-money laundering remains low in the sector and needs to be increased.

Table 60. Trainings organized by the FIU during 2020–2024

Date	Topic	Participants
30.03.2021	Introduction to the Financial Intelligence Unit, supervision, and reporting obligation	60
25.05.2021	Reporting obligation – indicators, shortcomings, risks in the accounting sector, including NRA	73
21.10.2021	Money laundering risk requires enhanced due diligence measures – Accountants' Conference	60
13.10.2022	The role of accountants in preventing money laundering and terrorist financing	60
24.11.2023	RUP.ee Accountants' Conference 2023	130
29.10.2024	General lecture on anti-money laundering for accounting students at the Tallinn University of Applied Sciences	45

Source: FIU

Although accountants and tax advisors do not move money directly, their role in preparing financial data is very important. They help companies understand their tax obligations, make business decisions, and demonstrate their financial position. Therefore, they play a key role in noticing when something in business structures or money flows seems suspicious and may indicate money laundering. Through their work, they see where money comes from and where it goes, and can assess the legality of transactions and monitor whether they comply with AML and counter-terrorist financing requirements, as well as adherence to applicable sanctions.

The main risk in the activities of accountants and tax advisors is serving suspicious or unclear clients, which involves several risk indicators. This includes fictitious transactions and services, such as goods brokerage without actual movement of goods or advisory services that are not genuinely provided but involve international money transfers. The greatest threat is the intentional involvement of an accounting firm or an individual accountant in money laundering using their own company. In addition, due to previous sector issues, there is a risk of tax fraud and complex money laundering schemes.

Significant vulnerability also arises from accountants' limited ability to identify and knowledge gaps, especially in cases related to e-commerce or foreign clients, where there is no possibility to verify the background of transaction partners. Lack of knowledge and necessary but expensive IT solutions also increase the level of vulnerability.

CASE STUDIES:

- The first example case highlights a situation where an accounting service provider identified that a client, an Estonian company, purchased a yacht using another foreign company's assets due to lack of own funds. Additionally, the ownership structure changed, with a new shareholder being a company from the United Arab Emirates together with a Romanian citizen as the ultimate beneficial owner.
- The second case involves a client's sudden turnover change: turnover reached millions of euros, and the annual report documentation was incomplete (missing invoices and contracts).
- The third case describes donations received by a non-profit organization (NPO), where it was impossible to identify donors or the exact use of funds, and the NPO was associated with several e-residents.

The accounting and tax advisory services sector has a medium level of vulnerability to money laundering and terrorist financing, mainly due to the sector's characteristics: many small businesses and sole proprietors may lack sufficient competence and resources to comply with the requirements of the MLTFPA.

Positive aspects include transaction traceability and strong compliance capabilities among larger service providers.

5.9. Real Estate Brokers

The level of money laundering vulnerability among real estate intermediaries is **above average**.

According to the MLTFPA, obliged persons in the real estate sector include individuals who mediate the purchase or sale of real estate, as well as those who mediate real estate lease transactions where the agreed monthly rent is at least €10,000. In Estonia, two active umbrella organizations operate in the real estate market, bringing together brokers and real estate agencies – the Estonian Chamber of Real Estate Agents (EKMK) and the Estonian Association of Real Estate Companies (EKFL).

As of 2024, there are approximately 475 real estate agencies in Estonia. 71 companies¹³² are members of EKFL. The EKMK register lists 1,062 brokers, of whom 216 are also entered in the Professional Register¹³³. In 2024, the sector's turnover was €57.4 million.

Membership in both umbrella organizations is voluntary, meaning there is no complete overview of market participants in Estonia. Anyone can operate as a real estate broker or establish a real estate agency without a professional certificate or license. Since virtually anyone can provide real estate brokerage services and there is no control over this, it is known that brokers operate in the market who are unaware of their obligations under MLTFPA and therefore do not comply with them. This significantly increases the vulnerability of the real estate brokers' sector.

Although the real estate brokers' sector is one of the least regulated sectors in terms of AML (no entry barrier), a positive aspect is the regulation of real estate transactions, where purchase-sale transactions are notarized and recorded in the land register. This helps ensure transparency, as all transactions are traceable

¹³² <https://www.ekfl.ee/liikmed/>

¹³³ <https://maakleritekoda.ee/maaklerite-register>

and documented, and allows authorities to monitor changes in ownership and the legality of transactions. Additionally, notaries are required to identify the parties to the transaction, reducing the possibility of anonymous or fictitious transactions. However, lease transactions are not notarized.

Supervision of real estate intermediaries is carried out by the FIU. The FIU actively engaged with the sector in 2020–2021. In 2020, the FIU conducted 10 on-site inspections in real estate agencies, identifying deficiencies in compliance with MLTFPA in nine cases. In 2021, two remote inspections were carried out. The main shortcomings were found in procedural rules, risk assessments, and application of due diligence measures. Four entities received orders to remedy deficiencies, and additionally, misdemeanor proceedings were initiated and penalty payments imposed. These measures are considered effective, as they achieved their purpose and companies brought their activities into compliance with the law.

The identified deficiencies in most inspected companies indicate the sector's low awareness of risks and its due diligence obligations. Due to this lack of awareness, the sector also submits very few reports (see Table 61).

Table 61. Reports submitted by real estate brokers to the FIU by type during 2020–2024

Type of report	2020	2021	2022	2023	2024
UTR		1			1
UAR			2		
STR	7	1	1		
ISR		2		1	
CTR		1			1
TFR		1			
TOTAL	7	6	3	1	2

Source: FIU

The FIU's expectations for fulfilling the reporting obligation are significantly higher regarding suspicion-based reports. Reports have been forwarded to law enforcement agencies (see table below).

Table 62. Reports forwarded to law enforcement agencies during 2020–2024

	2020	2021	2022	2023	2024
Real estate brokers	2	1	1		

Source: FIU

Estonia has ranked first¹³⁴ in Europe for real estate price growth over the past decade. However, high property prices make real estate increasingly attractive as a target for money laundering. Suspicious money entering the market drives property prices up—this is particularly relevant in Tallinn, where real estate prices are significantly higher. Moreover, the FIU receives more reports about suspicious real estate transactions than from real estate agents themselves.

¹³⁴ <https://arileht.delfi.ee/artikkel/120288352/graafikud-euroopas-esikohal-eestis-on-kinnisvarahinnad-kumne-aastaga-tous-nud-ule-200-protsendi>

RISK SCENARIOS:

- **The main risk scenario for Estonian real estate brokers** is the purchase of property using assets of criminal, suspicious, or unclear origin. For example, there was suspicion that **shell companies were used to buy real estate with assets of unclear origin**. Companies were granted loans in virtual currencies, which were exchanged into euros via virtual currency exchange platforms and transferred to company bank accounts through intermediaries. The funds received were then transferred to a notary's escrow account for property purchase.
- A second risk scenario may involve using real estate intermediaries' services to sell property that was previously purchased with **assets of unclear origin**.
- A third risk scenario may involve the **use of straw men in real estate transactions**.

The client base of real estate agents is generally lower risk—most clients are residents, and representation from high-risk jurisdictions and politically exposed persons (PEPs) is minimal.

5.10. Company Service Providers

The level of money laundering vulnerability for company service providers **is above average**. The CSP sector includes companies whose sole business activity is providing company services, as well as companies that primarily offer accounting and/or legal advisory services and additionally provide corporate services.

To provide trust management and corporate services in Estonia, a license must be obtained. The license is issued and compliance with the MLTFPA is supervised by the FIU. The number of licensed CSPs has decreased in recent years: as of 31 December 2020, there were 315 CSPs in Estonia, while as of 31 December 2024, there were 259. Market consolidation was partly driven by a sector-wide remote inspection conducted by the FIU in 2022, covering 322 companies. As a result of the inspection, about 30 CSPs voluntarily surrendered their licenses, and decisions to revoke licenses were issued to 13 more.

According to remote inspection data, 73% of CSPs provide address services, 45% offer company formation services, and 26% provide services related to share transfers. 18% of companies offer only trust management and corporate services, while about 70% of licensed CSPs also provide accounting, tax advisory, and legal services.

Since the 2021 risk assessment identified CSPs as a medium or high supervisory priority, the FIU focused on controlling this sector during the period covered by this report: two on-site inspections in 2020, three in 2021, four in 2022, four in 2023, and seven in 2024.

In almost all inspection procedures, deficiencies¹³⁵ in compliance with MLTFPA were identified (see Table 63). The FIU found shortcomings in risk assessments, procedural rules, and the application of due diligence measures, including identification of persons, beneficial owners, and the origin of funds. To address violations and deficiencies, the FIU issued orders for corrective actions during the reporting period, imposed penalty payment orders¹³⁶ on CSPs, and issued one misdemeanor decision in 2020 for operating without a license¹³⁷. The sector itself considers these measures effective and deterrent.

¹³⁵ Three companies relinquished their operating licenses during the observed periods as part of the supervisory procedure; therefore, no deficiencies were identified for them.

¹³⁶ 45 coercive payment orders were issued because the companies failed to complete the sectoral remote monitoring questionnaire sent in 2022.

¹³⁷ Penal Code § 372 (3), sum of €8,000.

Table 63. Statistics on inspections and their results under FIU supervision during 2020–2024

Type of supervision	2020	2021	2022	2023	2024
On-site inspection	2	3	4	4	7
Sector-wide remote inspection			322		
Company-specific remote inspection		1			
Number of on-site inspections where deficiencies in compliance with MLTFPA requirements were identified	2	2	4	2	6
Number of remote inspections where deficiencies in compliance with MLTFPA requirements were identified		0			
Deficiencies in risk assessment and risk profile	2	2	4	2	2
Deficiencies in procedural rules and internal control regulations	2	2	4	2	2
Deficiencies in due diligence measures	2	2	4	2	2
Deficiencies in fulfilling the reporting obligation	2		4	1	1
Deficiencies in data retention		1	4	1	2
Injunction to remedy deficiencies identified during supervision	2	1	1		2
Coercive fine				47	

Source: FIU

Additionally, inspection procedures have revealed that **CSPs do not understand their gatekeeper role** or its connection to preventing money laundering and terrorist financing. CSPs act as gatekeepers because they can create or control companies that may be used to conceal the ownership and movement of illicit funds and to evade sanctions. This significantly increases the sector's vulnerability level.

CASE STUDY:

According to information collected by the FIU, companies established through Estonian corporate service providers have been used abroad to commit crimes. For example, Estonian CSPs established three companies providing virtual currency services, which held FIU licenses. These companies were subsequently transferred to other individuals. In a foreign jurisdiction, a large-scale investment fraud occurred, involving companies that moved criminally derived funds in significant amounts to bank accounts opened abroad by Estonian virtual currency service providers (previously established by Estonian CSPs). The funds received by Estonian companies were then transferred to other foreign bank accounts belonging to virtual currency service providers operating in foreign countries. These foreign providers converted the assets into virtual currencies, which were then moved further across various blockchains. This case indicates that Estonian companies created and transferred by CSPs were likely used for money laundering.

FIU supervisory procedures indicate a high proportion of clients originating from high-risk jurisdictions. The service offered by TCSPs, which includes company formation, is often targeted at foreigners (e-residents and non-residents) and is therefore inherently vulnerable. The vast majority of the sector establishes business relationships and provides services without meeting the client in person, which increases anonymity-related risks.

In 2019, a virtual marketplace called ‘e-Residency Marketplace’ was created for e-residents, aiming to bring together reliable service providers with verified backgrounds. The marketplace currently includes 41 companies offering services such as company formation, registered address, and contact person services. A positive aspect is the cooperation between the FIU and marketplace members, for example through roundtables and training sessions.

Additionally, FIU supervisory procedures have identified that some CSPs allow invoices issued for their services to be paid by third parties, without identifying who these third parties are or why they are paying on behalf of others.

Limited awareness of risks and sector typologies is also reflected in the low level of reporting by the sector (see table below).

Table 64. Reports submitted to the FIU by CSPs by type, 2020–2024

Type of report	2020	2021	2022	2023	2024
UTR		1	1	3	5
UAR	6	5	7	18	16
STR	3		7	6	19
ISR			2	4	2
CTR			1		
TFR					4
Total	9	6	18	31	46

Source: FIU

The quality of reports submitted by CSPs varies greatly and depends on the submitter. Some CSPs consistently provide reports of uniform quality, making it clear why the FIU was notified and what actions the CSP itself took (e.g., terminated the client relationship). Excluding these, CSP reports often have recurring issues with formatting errors, such as missing or incorrectly indicated related persons or documents. 15% of reports are substantively flawed, including cases where the transaction description is incomplete or the content of the report is unclear, making it impossible to understand why a suspicion of money laundering arose.

The FIU has only started forwarding CSP reports to law enforcement agencies since 2024 (see table below). In previous years, no reports were forwarded.

Table 65. Reports forwarded to law enforcement agencies in 2020–2024

	2020	2021	2022	2023	2024
Company Service Providers					6

Source: FIU

Although the forwarding of reports has increased over the observed period, the sector still submits few reports. The FIU also sees various CSPs that, due to their risk appetite, client portfolio, and other reasons, should be submitting reports to the FIU but have not done so. Some Estonian CSPs have, both previously and during the observed period, established and transferred companies to high-risk virtual asset service providers and created and/or offered address services to shelf companies linked to gambling service provider schemes (miscoding schemes). None of the CSPs involved in these typologies have submitted reports to the FIU.

The sector continues to offer nominee director services, which allow concealment of actual controllers. Such services are prohibited under Estonian law, and offering them significantly increases the sector's vulnerability. The legal framework also creates confusion, as the MLTFPA lists services that, in practice, must not be provided—such as acting as a trustee or shareholder. Additionally, it is known that several companies operate without a license (estimated at about 40% of service providers¹³⁸), and the sector perceives insufficient effective control and sanctions by authorities regarding these companies. The vulnerability level is reduced by the fact that company formation services require identity verification either via ID card or through a notary. Although notaries only verify the person authorized to sign, most CSP clients have board members and beneficial owners who are the same. This is confirmed by a sector survey, according to which all respondents stated that they have fewer than 20% clients with complex structures. Furthermore, CSPs do not manage client assets, conduct transactions, or participate in clients' business activities.

The vulnerability level is increased by companies that allow payment for their services in virtual assets, as CSPs lack the capability to monitor virtual asset-related transactions during the business relationship and to verify who pays their invoices. According to sectoral remote monitoring, at least 12 companies use virtual asset wallets in their business activities, and based on the questionnaire sent to the sector, fewer than 10% of respondents settle payments in virtual assets.

The FIU has contributed to the sector through training sessions, notices, and typology reports. Between 2020 and 2024, the FIU conducted seven sector-specific trainings aimed exclusively at CSPs, with a total of 695 participants. In addition, several trainings were conducted for multiple sectors, including CSPs.

¹³⁸ <https://www.politsei.ee/et/uudised/politsei-alustas-tegevusloata-aeriuehingute-teenuse-pakkujate-suhtes-menetlusi-11039>

5.11. Lawyers

The level of money laundering vulnerability among lawyers is **medium**.

In Estonia, anyone can provide legal services, but only members of the Estonian Bar Association who meet the statutory requirements may use the title of lawyer. Lawyers do not have an exclusive right to provide legal services in Estonia—neither in court nor out of court—and the provision of legal advice is not separately regulated. Therefore, regulated legal services offered by lawyers differ from other legal services that are not subject to the same professional and ethical requirements.

As of the end of 2024, the Estonian Bar Association had 902 active members (a total of 1,154 members) working in 210 law firms.

The professional activities of lawyers are regulated by the Bar Association Act, internal rules, the Code of Ethics, and guidelines and instructions. The MLTFPA applies when a lawyer acts on behalf of and in the interests of a client in financial or real estate transactions and when a lawyer advises on planning or executing a transaction or performs official acts or services related to the activities listed in § 2(2)(1–5)¹³⁹ of the MLTFPA. Of the 210 law firms (as of December 2024), 88 provided such services—42% of all law firms—and can therefore be considered obliged entities. For the NRA survey, information was sent to law firms (139 firms in December 2024), and 134 firms responded to the questionnaire, a 96% response rate.

The law does not apply to cases where a lawyer assesses a client’s legal position, defends or represents them in court or other proceedings, including advising on initiating proceedings or after their conclusion in matters related to the services listed in § 2(2) of the MLTFPA. In addition, lawyers must comply with the International Sanctions Act when fulfilling anti-money laundering and counter-terrorist financing requirements.

¹³⁹ 1) The purchase or sale of real estate, businesses, or shares of companies.
2) Managing the client’s money, securities, or other assets.
3) Opening or managing payment, savings, or securities accounts.
4) Obtaining funds necessary for the establishment, operation, or management of a company.
5) Establishing, operating, or managing trusts, companies, foundations, or other entities without legal personality.

Risk scenario related to membership in the management body of a legal entity:

In 2024, the Bar Association's Disciplinary Committee handled a case where a lawyer offered a foreign person the service of acting as a management board member. The case involved seven companies and took place over several years during the observed period. The case illustrates how a lawyer may be vulnerable to suspicious or unclear activities when providing legal services or even become directly involved in them.

- The lawyer's client disappeared and could not be contacted.
- It was established that by failing to submit annual reports and interim liquidation reports as a management board member, the lawyer did not fulfill statutory obligations when providing legal services (even if clients did not raise complaints).
- If an auditor does not approve the annual report, this indicates possible deficiencies in the company's administration or documentation, for which the lawyer is also responsible as a management board member. If the auditor refuses due to disagreements, another auditor should be appointed. If no auditor approves the report, this points to shortcomings in the company's operations.
- According to the facts presented to the Disciplinary Committee, the client's mandate was to liquidate the private limited company.
- If the client's mandate is liquidation, this does not require the law firm to acquire a shareholding in the company. Providing services related to membership in the management body and shareholding entails responsibility for the lawyer and the law firm, which in turn involves risks.

The identified extensive failure to fulfill obligations raised the question of whether the lawyer was appointed to management bodies for **unlawful purposes (linked to clients' suspicious or unclear activities or even personally involved)** or whether the lawyer assumed too many tasks to manage effectively.

The Disciplinary Committee emphasized that membership in the management body and shareholding entails responsibility and risks for the lawyer and the law firm. **Extra caution and critical judgment are required in situations where a law firm acquires a shareholding in a company designated for liquidation, especially in companies not established by the lawyer or law firm, where they have not participated in operations and do not fully know the background.**

In the survey, only a small proportion (3%) of lawyers indicated that their clients include politically exposed persons (PEPs), individuals from high-risk jurisdictions, or companies with complex ownership structures. Notably, 26.87% of law firms provided legal services during the assessment period that included acting as a client's company director or management board member. Providing legal services involving membership in a management body increases money laundering vulnerability, particularly in cases involving foreign clients or complex structures. However, such services may also involve legitimate objectives such as liquidation, restructuring, or other lawful purposes, which are regulated by Bar Association guidelines and carried out under its supervision and do not automatically increase money laundering or terrorist financing vulnerability.

Estonian law firms providing cross-border services to foreign law firms often rely on data collected by the foreign law firm under § 24 of the MLTFPA when applying due diligence measures. This means Estonian lawyers do not apply due diligence to the foreign firm's end clients. Consequently, it is uncertain whether these end clients fall into high-risk categories. Since due diligence is applied at the end-client level by the foreign law firm, the actual money laundering and terrorist financing vulnerability inherent in such intermediary arrangements may remain hidden. Therefore, the actual number of high-risk clients using lawyers' services through such arrangements is likely higher than survey results suggest.

The MLTFPA applies to lawyers in limited cases. The supervisory role is fully carried out by the Management Board of the Estonian Bar Association, which oversees compliance with AML requirements across its membership through administrative procedures. The Disciplinary Committee has jurisdiction over disciplinary proceedings (including imposing sanctions) based on findings from the Management Board's supervision, as the Committee does not have independent authority to identify AML violations. The FIU has jurisdiction over misdemeanour proceedings.

It is important to note that supervision within the Bar Association has been coordinated between the Management Board and the Disciplinary Committee, which has occasionally raised questions in practice regarding competence and efficiency. Under the current MLTFPA, supervisory authority lies with the Management Board, while the Bar Association Act assigns disciplinary sanctioning authority to the Disciplinary Committee. This has created a situation during the assessment period where one body conducts supervision and the other imposes disciplinary sanctions, making Bar Association procedures more resource-intensive. The Bar Association is aware of this and is working to clarify and streamline processes to improve coordination and ensure effectiveness.

Since 2022, the Bar Association has applied a risk-based approach to monitoring compliance with AML requirements among its members, distinguishing firms engaged in transactions under § 2(2) of the MLTFPA. This demonstrates the Bar Association's commitment to improving its supervisory system. Although 2023 statistics showed that a significant portion of inspections (60%) were conducted in low-risk firms, the Bar Association has actively worked on refining its risk-based methodology to ensure greater focus on higher-risk areas related to money laundering and terrorist financing. During the observed period, investments were made in supervision, such as remote monitoring, and systematic measures were implemented to strengthen focus on higher-risk areas. The Bar Association has taken significant steps and continues to work toward making supervision sufficiently risk-based.

As of 31 December 2024, supervision of law firms within the Bar Association is carried out by a legal assistant at 0.5 FTE, half of which is dedicated to AML and sanctions oversight. Legal assessments are also provided by the office lawyer, and substantive legal expertise in supervision comes from the Management Board member responsible for the area. Recognizing the need to improve supervisory capacity and optimize processes due to critical resource shortages, the Bar Association has taken important steps. In 2025, it was decided to create a dedicated AML and sanctions specialist position, doubling the number of supervisory staff—a significant change demonstrating the Bar Association's commitment to strengthening supervision. Additionally, since March 2025, two Bar Association members have been appointed to actively address these key issues, ensuring the necessary attention to the area.

Given the large number of supervised lawyers and firms (210 firms and over 902 lawyers), the Bar Association is aware of resource needs. To address this, on-site inspections have been supplemented with remote monitoring since 2022, helping to use workforce more efficiently and expand the scope of inspections. These positive developments reflect the Bar Association's proactive efforts to improve quality and coverage of supervision.

Table 66. Statistics on inspections and their results within the Bar Association’s supervision in 2020–2024

Type of supervision	2020	2021	2022	2023	2024
On-site supervision (number of law firms inspected)	22	23	24	23	18
Remote inspections (questionnaire completed)	0	0	56	12	5
Number of on-site inspections where deficiencies in compliance with MLTFPA requirements were identified	4	1	1	15	9
Number of remote inspections where deficiencies in compliance with MLTFPA requirements were identified	0	0	8	12	5
Remote inspection – low-risk law firms	-	-	0	9	5
Remote inspection – medium-risk law firms	-	-	40	3	-
Remote inspection – high-risk law firms	-	-	16	0	-
Remote inspection – company-based	0	0	56	12	5
Deficiencies in risk assessment	1	0	0	10	8
Deficiencies in procedural rules/internal control regulations	0	1	0	9	8
Deficiencies in due diligence measures	0	0	0	1	2
Administrative measure in case of violation (requirement to rectify deficiencies)	4	1	9	27	14

Source: Bar Association

During 2020–2024, the Bar Association’s supervisory activities identified significant deficiencies in compliance with AML requirements. These deficiencies mainly relate to the application of due diligence measures (such as failure to identify beneficial owners), insufficient risk assessment, and procedural rules. It is concerning that reports of suspicious activity have been extremely rare. Therefore, it is important to focus on lawyers’ willingness to apply due diligence measures more effectively, as well as on further strengthening supervision.

In cases of AML violations, the Bar Association, as the supervisory authority, may impose disciplinary sanctions on a lawyer who is an obliged entity under the MLTFPA. Sanctions may include a reprimand, a fine payable to the Bar Association ranging from €64 to €16,000, suspension of professional activity for up to one year, expulsion from the Bar Association, or revocation of the right to act as a bankruptcy trustee for up to five years. All these sanctions can be applied for AML violations and may be imposed personally on the lawyer; additionally, a lawyer holding a management role in a law firm is also responsible.

During the observed period, the Bar Association did not identify violations constituting misdemeanours, and no sanctions under the Bar Association Act were imposed on lawyers or law firms, as deficiencies found during supervision were corrected within the prescribed timeframe (during the procedure). According to Bar Association representatives, the aim of supervision is educational—to raise awareness and encourage the elimination of deficiencies. While correcting deficiencies during the procedure is effective for short-term solutions, attention must also be paid to addressing systemic problems to prevent repeated violations in the future. The Bar Association continuously works to support lawyers and law firms in complying with AML requirements by providing guidance and training. In cases of more serious violations, it is important for the Bar Association to respond with appropriate measures, especially when these are part of a broader issue. Misdemeanour proceedings fall under the FIU’s jurisdiction. The Bar Association did not submit any

misdemeanour reports to the FIU during the assessment period. Cooperation and information exchange between the Bar Association and the FIU are essential to ensure consistent and effective supervision across the sector.

Table 67. Statistics on reports submitted by lawyers to the FIU in 2020–2024¹⁴⁰

Main activity	2020	2021	2022	2023	2024
Lawyers (Bar Association members, board)	7	6	19	9	9
CTR		1			
STR	6	3	6	3	4
UTR				1	3
UAR	1	2		1	1
ISR			13	4	1

Source: FIU

Lawyers' contribution to preventing money laundering and terrorist financing is significant. Although lawyers have a statutory obligation to report suspicious activities, the extremely low rate of suspicious activity reports highlights the need for systemic improvements. This indicates opportunities to enhance lawyers' ability to identify and assess potential warning signs in client behavior. One of the key factors that can improve reporting rates is the creation of specific guidelines and indicators for recognizing suspicious transactions and red flags. The absence of such guidance has led to uncertainty among lawyers in detecting suspicious behavior.

Discussions in working groups with Bar Association representatives confirmed that while a lawyer's initial impression of a client may raise doubts about the client's intentions, this does not automatically indicate money laundering suspicion. Such clients may not always enter into a business relationship or trigger due diligence measures, often due to a lack of awareness that the nature of the suspicion should be analyzed and, if necessary, reported to the FIU at the earliest stage. This underscores the need to improve awareness of FIU requirements. In addition to guidelines, the role of systems and tools is crucial. During the observed period, the sector lacked solutions to support monitoring client activities and comparing them with risk profiles. Tools such as automated checks against sanctions lists and politically exposed persons (PEPs) were also missing, which would simplify the detection of suspicious patterns and give lawyers confidence in fulfilling their obligations.

Since reporting is a cornerstone of the anti-money laundering system, its practical implementation significantly contributes to the overall effectiveness of the system and strengthens supervision. Cooperation between the FIU and the Bar Association is key to ensuring that lawyers have both the necessary knowledge and tools to meet their obligations. Regarding information availability, challenges include verifying foreign documents and the absence of a national register of politically exposed persons, which complicates identification. Although a beneficial ownership register exists, its data quality is low, and there is a lack of clarity regarding the timeliness of sanctions lists.

¹⁴⁰ See explanations of report types in the „Abbreviations“.

5.12. Notaries

The level of money laundering vulnerability among notaries is **medium**.

There are 100 notary positions in Estonia, of which 87¹⁴¹ were filled as of 2024. The most recent appointment of a notary took place in August 2024. The conditions for becoming a notary are regulated by the Notaries Act (hereinafter 'NotA'). To become a notary, one must first complete a two-year candidacy, which includes substituting practicing notaries. A vacant notary position is filled through a competition announced by the minister responsible for the field after consulting the Chamber of Notaries. The competition is organized by the Chamber's examination committee. Notaries operate independently or in shared offices, but each notary bears personal responsibility for their official activities. All Estonian notaries are members of the Chamber of Notaries, a public-law legal entity.

Activities related to preventing money laundering and terrorist financing (hereinafter 'AML prevention') are governed by a clear and functional legal framework: the AML Act, the International Sanctions Act, the Notaries Act, procedural rules and internal control regulations approved by the Chamber's General Assembly, and FIU guidelines.

Estonian notaries use the electronic information system e-Notar, through which all transaction-related queries are made. e-Notar stores query responses and all transaction-related documentation, including data and documents collected for AML prevention.

From an AML perspective, notaries are obliged entities primarily in two areas: real estate transactions and corporate transactions. Between 2020 and 2024, the number of real estate transactions ranged from 66,551 to 88,155. In 2024, a total of 66,792 real estate transactions were carried out. During the same period, corporate transactions averaged around 10,000 annually. Cash transactions account for a very small share of both types, as confirmed by an NRA survey among notaries and the number of CTR reports submitted¹⁴² to the FIU.

According to the Land and Spatial Planning Agency, the number of real estate transfer transactions per calendar year between 2020 and 2024 ranged from 51,107 to 71,718. Sales transactions accounted for 79.2–84.7% of all real estate transactions during this period. The annual total value of transactions ranged from €4.04 to €5.98 billion. The sector's vulnerability level is also influenced by the number of transactions involving foreigners¹⁴³. Between 2020 and 2024, transactions involving foreign sellers ranged from 3,718 to 4,910, and transactions involving foreign buyers ranged from 3,422 to 4,562.¹⁴⁴ The requirement for notarial certification of real estate sales illustrates the importance of the notary sector in AML prevention.

According to an NRA survey among notaries, AML due diligence measures are applied in notary offices not only by the notary but also by office staff, although at least 10% of notaries apply these measures alone. The survey was sent to all 87 notaries (December 2024), of whom 63 responded (72%). Notaries' exposure to clients requiring enhanced due diligence or strengthened measures under §§ 38 and 39 of the AML Act and procedural rules is low—approximately 80% of notaries encounter 0–10 such clients annually. In recent

¹⁴¹ The declining trend in the occupancy of notary positions has continued: as of 2020, 91 out of 100 positions were filled.

¹⁴² In 2024, 77 CTR reports were submitted, accounting for less than 0.1% of the number of transactions.

¹⁴³ This includes individuals who do not hold Estonian citizenship, including stateless persons or permanent residents with Russian citizenship, and private legal entities registered in a foreign country.

¹⁴⁴ Estonian real estate market in 2024: <https://maarium.ee/sites/default/files/documents/2025-02/Eesti%20kinnisvaratarg%202024.pdf>; in 2023: <https://maarium.ee/sites/default/files/documents/2024-02/Eesti%20kinnisvaratarg%202023.pdf>; in 2022: <https://maarium.ee/sites/default/files/documents/2023-02/Eesti%20kinnisvaratarg%202022.pdf>; in 2021: <https://maarium.ee/sites/default/files/documents/2022-02/Eesti%20kinnisvaratarg%202021.pdf>; in 2020: https://maarium.ee/sites/default/files/documents/2021-06/eesti_kinnisvaratarg_2020.pdf.

years, the share of clients from countries with higher terrorist financing risk¹⁴⁵ has also decreased; in 2024, such clients accounted for about 10% of transactions. The main reason for this decline is the reduced number of clients from the Russian Federation.

Supervision of notarial activities is carried out by the Ministry of Justice and Digital Affairs and the Chamber of Notaries. This includes supervision of compliance with AML requirements and related regulations. The Ministry has delegated AML-related supervision to the Chamber under § 5(2) of the Notaries Act and § 64(4) of the MLTFPA. Within the Chamber, only one person is responsible for organizing and conducting supervision on a daily basis, covering all aspects of supervision, not just AML measures. Considering the number of notaries and transactions, and the fact that administrative supervision covers more than AML compliance, this human resource is insufficient for effective supervision.

Supervision of notarial activities is carried out through regular inspections, extraordinary inspections, or follow-up checks. The Chamber's Board approves an annual inspection plan based on risk factors such as time since the last inspection, number of transactions, and turnover. Inspectors follow the Notarial Regulations and the Chamber's internal control rules. Inspectors cannot issue instructions or orders to notaries when deficiencies are found—this authority lies only with the Ministry and the Chamber's Board. The e-Notar system helps ensure proper document storage, facilitating supervision.

Between 2020 and 2024, a total of 15 administrative inspections were conducted; no inspections were carried out in 2020–2021 due to the COVID-19 pandemic. During the observed period, supervision highlighted deficiencies in notarial work and provided recommendations for improvement. For example, one inspection revealed inconsistent and insufficient application of AML measures, leading the Chamber's Board to order the notary to undergo additional training and organize training for office staff on AML measures.

The Chamber's Board or the Ministry may issue instructions or orders that are binding on notaries. If a notary fails to comply, the Ministry may initiate disciplinary proceedings, and the Chamber's Board may propose initiating a disciplinary case. Possible disciplinary sanctions include reprimand, fine, and removal from office. No disciplinary sanctions were imposed on notaries during 2020–2024. The FIU may impose penalties (i.e., fines in misdemeanor proceedings) for violations under Chapter 10 of the AML Act, but none have been imposed to date. Under § 54(1)(10) of the MLTFPA, the FIU is responsible for handling misdemeanors under the Act. Considering that a notary, as an obliged entity under the AML Act, is a natural person and given the potential fine amounts, these fines are significant¹⁴⁶ and sufficiently deterrent.

Money laundering offences are punishable under criminal law, but no criminal proceedings have been initiated against notaries. If a conviction becomes final, the minister responsible for the field removes the notary from office. During criminal proceedings, the prosecutor may request the suspension of a suspect or accused notary, and the corresponding court order is also sent to the workplace. Considering that initiating criminal proceedings against a notary can cause significant reputational damage, the risk of intentional money laundering offences among notaries is very low. The personal liability mechanism applicable to notaries encourages compliance with statutory obligations, including identifying suspicious transactions and fulfilling AML requirements, thereby helping to prevent potential violations.

¹⁴⁵ https://fiu.ee/sites/default/files/documents/2024-09/Lisa.%20K%C3%B5rgema%20terrorismi%20rahastamise%20riskiga%20riikide%20nimekiri_18.09.2024.pdf

¹⁴⁶ Depending on the offence, a fine of up to €1,000,000 may be imposed, or an amount corresponding to up to twice the profit gained or loss avoided as a result of the offence.

Notaries are not required to conduct background checks on employees—they hire staff at their own responsibility and risk. However, both notaries and notary office employees are subject to a confidentiality obligation under the Notaries Act regarding information obtained in connection with official activities.

Notaries are required to complete periodic legal continuing education, compliance with which is checked every three years. AML-related training for notaries and notary office staff is organized by the Chamber of Notaries.

Table 68. Training offered to the sector in 2020–2024

Date	Topic	Participants
18.02.2022	Risks in the sector and reporting obligations, and MONEYVAL	73
25.05.2022	Money laundering risks and reporting obligations	80
17.02.2023	Prevention of money laundering, prevention of terrorist financing, international financial sanctions	180
12.04.2024	Presentations to notaries (reporting, trends, sanctions, and TF)	103
04.11.2024	Training on submitting reports related to the Innoprojekt	10

Source: Chamber of Notaries

Between 2020 and 2024, five anti-money laundering training sessions were organized, three of which were conducted by FIU, who consider notaries to be one of the most trained sectors. Despite this, supervision has revealed that the knowledge acquired in these trainings is not consistently applied in daily work. The main issue with the lack of risk awareness is the absence of control over the training obligations of notary office employees – only the training of notaries is monitored, neglecting the knowledge level and currency of the employees. Although notaries are required to undergo training, supervisory checks have shown that some notaries only meet the minimum requirements for preventing money laundering. This creates a situation where a significant portion of the personnel involved in transactions may not be sufficiently trained, hindering effective money laundering prevention.

Table 69. Number of reports submitted by notaries to FIU by type of report¹⁴⁷ in the years 2020–2024

Notaries	194	172	183	168	173
Year	2020	2021	2022	2023	2024
CTR	75	58	65	68	77
STR	50	50	29	26	22
UTR	41	44	51	58	48
UAR	8	11	7	5	10
TFR-1	18	8	15	8	7
TFR-2	2				
ISR		1	16	3	9

Source: FIU

Between 2020 and 2024, the number of reports submitted by notaries to FIU has remained stable, ranging from 168 to 194. Compared to other professionals, notaries are at the top in terms of the number of reports submitted, indicating a high level of awareness of the reporting obligation. This is also confirmed by the fact that over the five years, at least 70% of notaries have submitted a report to FIU each year. Considering that the notaries' involvement in cases requiring reporting also depends on the notary's area of work, this is a very high indicator. However, alongside the total number of reports, the proportion of reports submitted with deficiencies has also increased, reaching 54%¹⁴⁸ in 2024.

Table 70. Proportion of problematic reports submitted by notaries to FIU

	2022		2023		2024	
	Number of reports	% of problematic	Number of reports	% of problematic	Number of reports	% of problematic
Notaries	48	41%	36	36%	52	54%
Missing supporting documents	16	14%	16	16%	5	5%
Content errors (incomplete transaction description, unclear content)	8	7%	8	8%	14	15%
Form errors (e.g. persons not specified)	24	20%	12	12%	33	34%

* When calculating the proportion, CTR reports were excluded from the total number of reports, as they are primarily analyzed in bulk.

Source: FIU

Information contained in reports submitted by notaries has been used in materials forwarded to Estonian investigative authorities every year during the evaluation period. In 2020, a restriction was placed on a transaction and property based on a report submitted by a notary, resulting in the suspension of an apartment ownership transfer transaction. It is positive that notaries are active in submitting reports, and their reports are valuable to FIU, contributing to the suspension of specific suspicious transactions.

¹⁴⁷ See explanations of report types in the „Abbreviations“.

¹⁴⁸ Reports for which no additional documents have been submitted or which contain content or form errors.

Table 71. Reports made by FIU to Estonian law enforcement agencies

	Reports made to Estonian law enforcement agencies 2020-2024				
	2020	2021	2022	2023	2024
Notaries	55	16	25	18	20

Typologies of vulnerabilities in the notary sector:

- Real estate transaction involving foreign legal entities: A foreign entity wishes to acquire real estate in Estonia, with a structure that has an unjustifiably large number of levels, including entities established in various offshore jurisdictions. The origin of the funds used for the purchase is described as an intra-group loan. For such entities, identifying the ownership structure and the ultimate beneficial owner is challenging (public registers are often lacking in offshore countries). The movement of the loan through several different entities within the same group complicates the identification of the origin of the funds.
- Acquisition of shares in private limited companies and establishment of private limited companies by foreign residents, including residents of high-risk countries. These individuals have no apparent connection to Estonia and lack an office or employees in Estonia. Such transactions may also occur solely through a representative based on a power of attorney, which means the notary has no direct contact with the client, and additional explanations from the client are mediated.

The vulnerability level of the sector is primarily increased by the limited effectiveness of supervision, the challenges in imposing administrative penalties, and the sector's low risk awareness.

6. ML Threats and Vulnerabilities of Virtual Currency Providers

In Estonia, it is possible to apply for a virtual currency service provider (hereinafter “VASP”) license, which allows the provision of four services: virtual currency wallet service, virtual currency exchange service, virtual currency transfer service, and services related to the issuance of virtual currency. Until the end of 2024, licenses were issued by the FIU, and from 2025 onwards, this is done by the FSA. The following umbrella organizations are associated with VASPs in Estonia: Web3 Chamber, Estonian Digital Asset Association, and NPO FinanceEstonia.

Several laws concerning VASPs were amended between 2020 and 2024, resulting in the addition of services that can be offered¹⁴⁹ with a license. Additionally, the requirements for obtaining a VASP license have been strengthened, leading to a decrease in both the number of VASP license applications and the number of active licenses in Estonia.

The risk assessment evaluated the risks associated with both Estonian VASPs (including by service type) and virtual currencies in Estonia. In terms of service volume, the most popular services among Estonian VASPs are the virtual currency wallet service, virtual currency exchange services, and transfer service (see table 73), which also carry the highest risks.

The risks in the VASP sector have decreased compared to previous periods. The residual risk level in the VASP sector is **medium**.

The level of money laundering threat in the sector is **above the average** for both virtual currencies and VASPs. Virtual currencies continue to be a significant means of concealing criminal proceeds. The main threats arise from the use of virtual currencies for criminal purposes, rather than from the threats posed by Estonian VASPs. **As of 31.12.2024, there are 42 virtual currency service providers in Estonia.** The overall risk level of service providers with an Estonian license has decreased compared to the years 2017–2019, but the risk has concentrated around service providers serving online casinos. Reports and external inquiries about market participants are on a downward trend, which may be due to the decrease in the number of market participants and improved risk awareness. There are still issues with compliance with the obligation to identify clients and ascertain the origin of clients’ funds.

Overall, the number of market participants with an Estonian virtual currency service provider license has remained smaller, and the decrease in information and external inquiries about them indicates a lower risk level. However, the risk has concentrated among a few market participants. Some Estonian licensed virtual currency service providers offer services to crypto casinos, indicating a higher-than-average risk level.

The level of vulnerability to money laundering in the sector is **above the average** for both virtual currencies and VASPs. Estonia has taken significant measures to reduce the level of vulnerability of VASPs. For example, cooperation and understanding of risks have improved, and several legislative changes have helped strengthen norms. Additionally, mandatory reporting for VASPs has been established since 2024.

¹⁴⁹ Specifically in the chapter “Changes in Virtual Currency Sector Licenses in the Period 2020 – 2024”.

6.1. Description of the Methodology

To assess virtual currency service providers, the latest version of the World Bank’s assessment module for VASPs was used. This module focuses on virtual currencies and Estonian licensed VASPs that offer services falling under the FATF definition (e.g., virtual currency wallet service, transfer service, exchange service). The assessment module allows for the evaluation of threats and vulnerabilities at the national level and the analysis of risks across different services according to the type of license.

Table 72. Module used for the assessment of the VASP sector

Sector	Assessment module
VASPs	Virtual Assets and Virtual Asset Service Providers (2025)

Threats and vulnerabilities associated with each service include various aspects that may affect the security and reliability of the service. Firstly, there is a threat that criminal proceeds may enter the service sector, enabling money laundering or other illegal activities. Additionally, it is necessary to consider the possibility that Estonian VASPs may be exploited by criminals, including the movement of assets associated with the dark web through Estonian VASPs. Furthermore, fraud and cyber-attacks, which may directly affect the service or occur through it, are also threats.

When assessing the vulnerability of each service, the inherent vulnerability associated with the service or product was analyzed, such as the decentralization of the system, the provision of services with higher-risk privacy coins, inadequate and insufficient transaction monitoring and tracking capabilities, and limited understanding of the money laundering and other risks associated with the service. On the other hand, the potential shortcomings of the prevention system were analyzed and assessed, such as the scope of legislation and supervisory capacity, the level of risk awareness among market participants, and their deficiencies in the process of identifying clients and applying due diligence measures, the frequency of reporting, and the quality of reports, among others.

The risk assessment used both quantitative data, such as the volume of services, client profiles, and international connections (including the proportion of clients from high-risk countries), as well as qualitative expert assessments and feedback from market participants (including the effectiveness of the regulatory framework and supervision), as well as risk typologies observed in the sector.

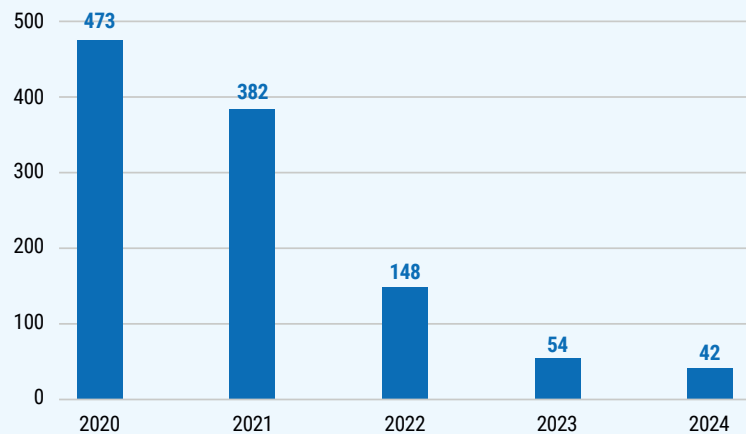
6.2. Regulatory Changes in the VASP Sector

1. Change in the number of VASPs sector licenses in the years 2020 – 2024

The requirements for entering the VASP market are significantly more effective compared to previous periods. According to the national risk assessment (NRA) conducted in 2021, the significant risks in the VASP sector were inadequate requirements for license applicants, short control time for market entry, hindered on-site supervision, actual non-connection with Estonia, rapid growth in the number of service providers, and the very different quality of due diligence measures among market participants. Consequently, several amendments to the MLTFPA were introduced in the period 2020–2024, significantly strengthening the rules for entering the VASP market, i.e., the requirements for applying for a license. This is also one of the main

reasons why the number of VASP licenses in Estonia has significantly decreased. **The improvement of the requirements for issuing VASP licenses and the implementation of more effective supervisory measures have significantly reduced the number of VASP licenses, which in turn has led to a reduction in the money laundering and terrorist financing risks in the sector in Estonia.**

Figure 15.
Number of VASPs as
of the end of the year
in the period 2020–2024



Source: FIU

In 2024, the composition of virtual currency service providers was relatively stable compared to previous years. During 2024, 13 VASPs lost their licenses (compared to 732 VASPs in 2021). As of the end of 2024, there were a total of 42 VASPs licensed in Estonia (see Figure 15).

Several significant legislative changes concerning VASPs allowed for substantial sector reorganization. In 2020, the FIU revoked a total of 1808 VASP licenses. This market reorganization was necessary to reduce the risks posed by fraud and money laundering cases involving Estonian-licensed VASPs. The 2021 risk assessment and various FIU analyses highlighted that a significant number of Estonian VASPs were owned by foreign entities and had only a formal connection to Estonia. The 2020 amendment to the MLTFPA the requirement that the service providers' place of business and management must be located in Estonia. As a result, the VASP sector was cleared of service providers with only a nominal connection to Estonia.

On March 15, 2022, an amendment to the MLTFPA came into force, which, among other things, introduced heightened standards for VASPs' IT systems, the competence of management and contact persons, the need for internal audits, and a significant increase in capital requirements. The capital requirement helped mitigate risks in Estonia that had already materialized or were about to materialize globally. For example, in 2023, a VASP that held a license in Estonia went bankrupt due to liquidity problems (unable to pay out virtual currencies to clients).¹⁵⁰ This case demonstrates the importance of VASPs having the necessary capital to protect clients from losing their virtual currencies. IT system requirements were updated in the law because IT risks in the VASP sector have increased year by year, and there have been cases in Estonia where cyber threats have materialized, resulting in significant losses of virtual currencies by Estonian VASPs.

Until the aforementioned legislative amendment, the MLTFPA defined only two virtual currency services – virtual currency exchange service and virtual currency wallet service. The amendment expanded the definition of virtual currency, resulting in the addition of new service offerings (virtual currency transfer service, ICO). Considering that the VASP sector is constantly evolving and new services frequently enter the market, it is

¹⁵⁰ <https://ekspress.delfi.ee/artikkel/120203484/kohus-kuulutas-valja-klientidele-u-le-200-miljoni-euro-volgu-jaanud-tallinna-kruptoari-pankroti>

important to assess whether new services entering the market meet the definition of a VASP and require a VASP license according to the applicable law. This helps further mitigate the money laundering and terrorist financing risks associated with VASPs.

In 2023, the European Union enacted Regulation (EU) 2023/1114¹⁵¹ on crypto-asset markets (commonly known as the MiCa Regulation), which established uniform rules for market participants in the European Union to operate in the crypto-asset market. The resulting amendments to national law were established in the Crypto Asset Market Act (KrüTS), which came into force on 01.07.2024.

Under the Crypto Asset Service Providers Act (KrüTS), the supervision of crypto asset services in Estonia is gradually transitioning from the FIU to the FSA. Until the end of 2024, FIU issued licenses to VASPs and will oversee the issued licenses until 30.06.2026. Service providers without a FIU license must apply for a license from the FSA starting from 30.12.2024, and the FSA will also supervise these licenses.¹⁵² The entry into force of KrüTS may further reduce the number of VASPs in Estonia, as in addition to supervisory changes, there will also be changes in the substantive requirements for obtaining a license (e.g., requirements established in the DORA regulation).

If the MLTFPA identified four types of virtual currency services, the Crypto Asset Services Act (KrüTS) recognizes ten types of services. The list of services requiring a license now includes, for example, executing orders related to crypto assets on behalf of clients, receiving and transmitting orders on behalf of clients, providing advice on crypto assets, and managing crypto asset portfolios.¹⁵³

From January 17, 2025, the European Union regulation on digital operational resilience for the financial sector (DORA regulation) will apply. The aim of implementing the DORA regulation is to achieve a high level of digital operational resilience for crypto asset service providers and asset-based token issuers, reduce the risk of financial disruptions and instability, and thereby increase the protection of clients, crypto asset owners, and investors. This indicates that VASPs have had issues with protecting clients' assets, and the EU has mitigated these risks through the DORA and MiCa regulations.

One reason for changing the supervisory authority is to ensure more effective protection of clients' assets and to mitigate IT risks in the VASP sector. The risk for VASP clients of losing their virtual currencies held by VASPs has increased year by year, primarily due to IT risks.

Due to the entry into force of the KrüTS and the DORA regulation, it is necessary to pay greater attention to explaining the new requirements to VASPs with an Estonian license and to those companies planning to apply for a license. Previous supervisory practices have shown that close cooperation with market participants and representative organizations, as well as training and information sessions, have played a significant role in the successful implementation of new requirements by VASPs. Such activities also help to reduce the vulnerability level of VASPs, as their knowledge of the new requirements increases.

As a result, the risk mitigation measures related to VASPs by the Estonian state have become significantly more effective year by year and are currently at a very good level. The improvement of these measures has helped to reduce the threat and vulnerability level of money laundering and terrorist financing for VASPs with an Estonian license.

¹⁵¹ <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32023R1114>

¹⁵² <https://www.fi.ee/et/blogi/mis-muutub-kruputoettevotete-jarelevalves>

¹⁵³ <https://www.fi.ee/et/blogi/mis-muutub-kruputoettevotete-jarelevalves>

2. VASPide kohustuslik regulaarne aruandlus ndatory Regular Reporting for VASPs

The mandatory regular reporting for VASPs has contributed to mitigating risks in the VASP sector. On December 16, 2023, a regulation by the Minister of Finance came into force, establishing a reporting obligation for VASPs with an Estonian license. According to the reporting obligation, VASPs must submit the following data for each quarter: general information, a report on due diligence measures, a report on the virtual currency services provided, a report on clients' assets, a balance sheet, and an income statement. The information collected through these reports allows the FIU and supervisory authorities to enhance strategic analysis and improve supervision of the VASP sector, as well as to avoid and prevent risks. As a result, Estonia has a continuously updated overview of what is happening in the VASP sector and its risks, enabling the implementation of appropriate risk mitigation mechanisms.

3. Changes in the Application of Due Diligence Measures – Travel Rule

In June 2019, the Financial Action Task Force (FATF)¹⁵⁴, the international standard-setter for anti-money laundering and counter-terrorist financing, extended the so-called travel rule requirement, which applies to payment services, to virtual currency service providers. In 2022, an amendment to the MLTFPA came into force, establishing an obligation for VASPs to apply the travel rule requirements. According to the amendment, virtual currency service providers must collect data on the originator and recipient of the virtual currency transfer when executing a transaction. This is an additional due diligence requirement that significantly affects the ability of VASPs to identify the parties to transactions. This requirement is directly related to the vulnerability of VASPs, specifically the application of due diligence measures, as it effectively mitigates the risks of money laundering and terrorist financing. The fact that a risk-mitigating measure has been enacted at the legislative level does not mean that this requirement is immediately applicable and achieves its full purpose. No supervisory procedures have been conducted for VASPs that focus on the proper implementation of the travel rule.

Globally, it has been noted that it remains challenging to implement the travel rule requirements, as no international agreement on uniform standards has been reached, making this not a problem unique to Estonia. In responses to the NRA expert group's questionnaire, most representatives of Estonian VASPs also pointed out that the implementation of the travel rule principle is very challenging. Specifically, it is difficult to identify the owner of the virtual currency wallet on the other side of the transaction. Currently, the travel rule requirements are formally met – the user enters their own or a third party's data as the recipient or payer of the virtual currency, but the actual connection between the virtual currency wallet and the person is not identifiable. The requirements are considered met if the client confirms that the data is correct, but this does not prevent the client from making transfers to a foreign virtual currency wallet, confirming that it belongs to them, or receiving funds from a foreign virtual currency wallet. This indicates that VASPs are vulnerable in the implementation of the travel rule, and there is a risk that Estonian VASPs may be used for money laundering or terrorist financing, as VASPs are unable to implement the travel rule requirements at the level intended. **VASPs need effective systems to ensure that virtual currencies move only to those individuals whose data has been declared to the VASPs. Increasing cooperation between the public and private sectors, both in Estonia and globally, will also contribute to the successful implementation of the travel rule.**

¹⁵⁴ Financial Action Task Force.

6.3. Estonia as a Transit Country for Virtual Currencies

The highest risk of money laundering and terrorist financing for VASPs with an Estonian license is associated with criminal activities occurring in foreign countries. The FIU already highlighted in 2021 that **Estonia is a transit country for the movement of virtual currencies.** The 2022 MONEYVAL assessment also found that Estonia encounters money laundering risks primarily through crimes committed abroad.

The 2022 FIU study on VASPs indicated that the sector is clearly concentrated in the hands of a few large service providers in terms of service volume and clients. More than 85% of the turnover in the virtual currency service sector was generated by 15 service providers (from July 2020 to July 2021). Approximately 83% of the virtual currencies received by these 15 service providers were also moved out of Estonia. Comparing the years 2024 and 2021, the characterization of the Estonian VASP market has not changed: Estonia remains a transit country, as blockchain analysis software shows that most of the virtual currencies received in Estonia also move out of Estonia.

In 2024, Estonian clients made up only 2% of the active clients of VASPs, and the transaction volume of Estonian residents accounted for 5% of all transactions. It is still evident from the reports of suspicious transactions related to money laundering and terrorism financing submitted to the FIU that **most of the reports** made by VASPs **do not concern Estonian individuals or have a weak connection to Estonia.** The same situation applies to foreign inquiries submitted to FIU, where, in addition to the weak connection of individuals to Estonia, the predicate offense is seen to have occurred abroad. The statistics on visits to the websites of Estonian VASPs also show a very small proportion of Estonian clients. Blockchain analysis software indicates that the inflows and outflows of VASP transactions are roughly the same. This previous statistic confirms that Estonian VASPs are used primarily for transit purposes, i.e., for **layering virtual currencies.**

In 2023, there was a case in Estonia where it was found that assets related to an investment fraud were transferred to an account opened with an Estonian VASP, which was opened based on forged documents. There were no other connections to Estonia. Additionally, in the same year, there was a case where an individual suspected of committing fraud abroad had an account with an Estonian virtual currency service provider, and there was a reasonable suspicion that the assets in the account originated from criminal activity.

Foreign inquiries about active Estonian VASPs to FIU are becoming fewer. More than half of the foreign inquiries received were related to VASPs that have lost their licenses. Most of the foreign inquiries concern individuals with foreign residency who have accounts with Estonian VASPs. The main topics in the foreign inquiries were individuals involved in drug sales or fraud.

The statistics on mutual legal assistance requests received by Estonian investigative authorities show that the number of mutual legal assistance requests related to Estonian VASPs has significantly decreased. In 2022, Estonian law enforcement agencies received 115 mutual legal assistance requests, which accounted for 12% of all submitted requests. In 2023, Estonian law enforcement agencies received 230 mutual legal assistance requests related to VASPs (10% of all mutual legal assistance requests). In 2024, significantly fewer mutual legal assistance requests were received compared to previous years – 19 requests (13% of all mutual legal assistance requests). Over the years, most mutual legal assistance requests have been related to fraud. The decrease in the number of mutual legal assistance requests is consistent with the fact that the number of VASP licenses has also significantly decreased from 2021 to 2024.

According to the responses to the expert group's questionnaires, Estonian residents prefer to use global platforms (the five most popular were Binance, Coinbase, Bybit, HTX, OpenSea), which offer a wider range

of services and often lower service fees. The share of VASPs in the total turnover of cross-border payments by credit institutions in 2024 was about a quarter (reference to the financial institutions working group), and the total turnover was 33.5 billion euros, which is equivalent to the sector's turnover in 2024. Considering the size of the turnover and knowing that only a few Estonian VASPs have accounts with Estonian credit institutions (and even then, only for administrative payments), it can be concluded that **a significant portion of the turnover is with VASPs licensed abroad**. From the perspective of law enforcement agencies, this contains certain risks. This means that foreign service providers generally do not report risk-based and suspicious transactions to FIU. All of this, in turn, makes it difficult to detect and prevent criminal activity from the perspective of both money laundering and terrorist financing.

Since there are few Estonian clients in Estonian VASPs, the main information gap is the activity of Estonian clients with VASPs licensed in other countries, as this data is not collected as part of mandatory reporting.

6.4. Risks and Volume of the VASPs

The turnover of VASPs from 2020 to 2024 is shown in Figure 16. Over the past three years, the turnover has grown significantly. The decline in turnover in the first half of the period can be explained by the significant reduction in VASP licenses, which included the loss of licenses by a few major market participants. At the end of 2023, the sector's turnover began to grow as both the global market prices of virtual currencies and the popularity of cryptocurrencies were on a strong upward trend. Additionally, the growth in the activity of market participants and the continuous improvement in data collection, including the mandatory reporting that began in 2024, have contributed to the quality of data on turnover volumes.

Figure 16.
Turnover of VASPs from
2020 to 2024 (billion €)



Source: FIU.

Based on mandatory reporting, the turnover across services in 2024 was 32 billion euros¹⁵⁵, and the total number of clients at the end of the last quarter was 1.64 million, of which slightly over 0.7 million were active service users. Table 73 shows that Estonian VASPs mainly offer wallet services, various exchange services, and transfer services. Therefore, the risks are also divided among these popular services. There are no virtual currency ATMs in Estonia; the last one was closed in 2023.

¹⁵⁵ Summarizing across services, there may be double counting.

Table 73. Virtual Currency Services Provided 2020–2024

Provided virtual currency service	Transaction value (billion €)	Number of clients as of last quarter
Virtual currency wallet service	9.79	128,000
Service for exchanging money for virtual currency	5.63	212,000
Service for exchanging virtual currency for money	5.57	127,000
Service for exchanging virtual currency for virtual currency	5.28	128,000
Transfer service (without changing the currency)	5.26	87,000
Other virtual currency service	0.69	53,000
Organizing an offering or sale	0.21	260
Financial service related to an offering or sale	0.00 ¹⁵⁶	470

Source: FIU

Considering the transaction volume in the VASP sector, the threat level for money laundering, terrorist financing, and sanctions evasion is high and is primarily concentrated on client relationships that Estonian VASPs have established with legal entity clients (correspondent relationships with other VASPs/financial institutions and client relationships with gambling operators).

The analysis results for 2024 based on mandatory reporting showed that only a few legal clients in offshore areas generate significant turnover, concentrated with a few service providers. For example, in the case of virtual currency wallet services, the service volume with Curacao clients accounted for 54%, and for transfer services (without changing the currency), it accounted for 31% of the total volume of the mentioned service. Across all services, the number of clients was less than 0.1%. Among the clients with higher turnovers in offshore areas were also the Isle of Man, Cyprus, Seychelles, British Virgin Islands, Vanuatu, etc. In several offshore areas, there were no individual clients at all. The mentioned offshore areas are associated with remote gambling operators offering crypto services (hereinafter “crypto casinos”).

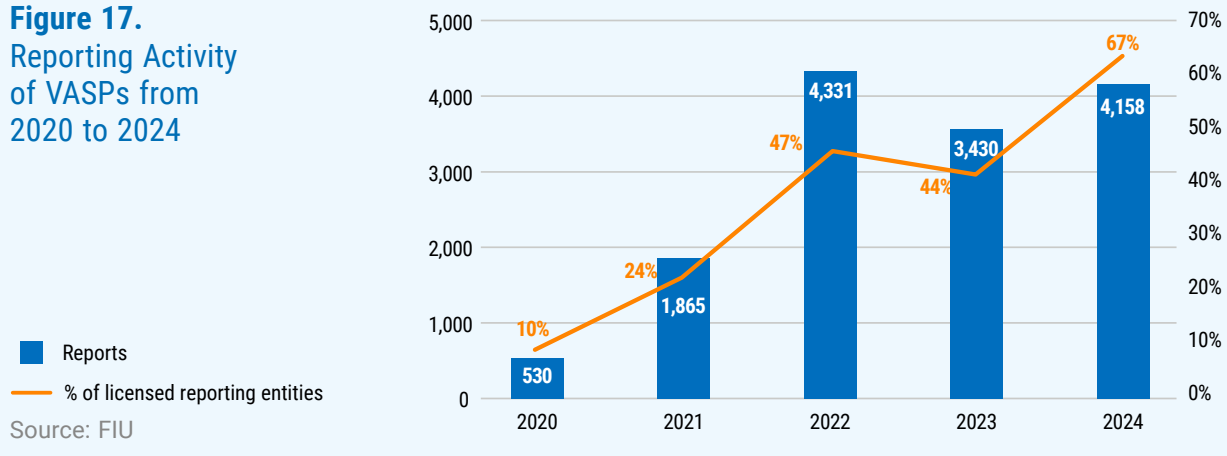
The VASP with the highest service volume accounted for 76% of the virtual currency wallet service (highest transaction value). Mainly, the clients of this VASP are a few legal entities, of which 26% were residents of Curacao, whose turnover accounted for 68% of the VASP’s turnover across services. The largest number of clients for the largest VASP was from Cyprus (37%). This means that the money laundering and terrorist financing risks realized by this market participant strongly affect the entire Estonian VASP sector.

6.4.1. Reporting activity of VASPs

The reporting activity and quality of VASPs have increased (see Figure 17), and VASPs are the second-largest reporters to the FIU, with their reports accounting for nearly a third of all reports in 2024. Among the suspicious transaction reports submitted by VASPs, significant typologies include fraud, identity theft, forged documents, credit card fraud, and the dark web. The analysis of the reports shows that topics related to fraud and identity theft clearly dominate. There are relatively few topics in VASP reports that are derived from transaction patterns and are harder to detect (e.g., connections to drugs, tax evasion, human trafficking, child pornography, etc.).

¹⁵⁶ Transaction value: €18,000.

Figure 17.
Reporting Activity
of VASPs from
2020 to 2024



The increase in the number of reports and the improvement in quality indicate that the awareness of VASPs licensed in Estonia about money laundering and terrorist financing risks has significantly improved year by year. However, there is still room for improvement in the quality of reporting, and the expectation is for accurate, suspicion-based reporting, considering the large volume of the sector and the international nature of transactions and clients.

According to Chainalysis¹⁵⁷ data, the share of illegal transactions in the total volume of crypto assets was 0.14% in 2024. Based on the proportions mentioned in the report (0.14–1%), the share of illegal transactions by Estonian VASPs in the total volume should range between 45–320 million euros. For comparison, the total amount of transactions mentioned in all reports submitted by VASPs to FIU in 2024 was 230 million euros (converted to euros). The total amount of reports falls within the range mentioned in the Chainalysis report, but there are still high-turnover VASPs that are unable to sufficiently detect illegal transactions, and there is a significant discrepancy between the volume of services provided and the amounts mentioned in the reports.

6.4.2. Risks of virtual currencies in Estonia related to crime

Due to effective supervision and the implementation of enhanced due diligence measures, the use of VASPs licensed in Estonia for criminal activities is not so easy. Over the years, the VASP sector has seen an increase in the activity of submitting suspicious transaction reports related to money laundering and terrorist financing and improved cooperation with state authorities. VASPs actively participate in training and information sessions and also organize conferences/training with the help of umbrella organizations. However, the risks of money laundering and terrorist financing related to virtual currencies and VASPs have not disappeared from Estonia. Therefore, the risk of money laundering and terrorist financing in Estonia is transferred to virtual currencies as a means to be used for criminal purposes. Legislative changes affecting VASPs have helped reduce risks in the sector, but the **risk assessment still showed that the threat level related to virtual currencies in Estonia is high, especially due to the possibilities of using them for criminal purposes.**

In Estonia, virtual currencies are primarily used in the following types of crime: fraud, cybercrime, organized crime, drug-related crime. Additionally, Estonian crime is characterized by the imitation of international trends, and the general trend is the increasing use of decentralized finance (also abbreviated as DeFi) applications. To the best of my knowledge, there are no DeFi platforms managed from Estonia, so anti-money laundering supervision of these platforms is not within the competence of Estonian supervisory authorities.

¹⁵⁷ Chainalysis, <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>

6.4.3. Use of DeFi

DeFi is a crypto-technical development, and it is wise to pay attention to its changes and potential associated risks in a timely manner. Unfortunately, decentralized finance applications do not fall within the scope of FATF recommendations. In the updated VASP guidance published in June 2023, FATF confirmed the increasing global use of DeFi protocols and identified it as a growing risk. One reason why criminals use DeFi solutions is that it makes it more difficult for law enforcement agencies to identify the origin and movement of funds. According to the responses to the expert group's survey among VASPs operating under an Estonian license, 68% of respondents found that the share of DeFi solution users has increased over the past three years. The perception of Estonian VASPs aligns with global trends, so it is necessary to pay heightened attention to the development of DeFi risks.

In parallel with the use of DeFi, there is a prevailing trend in Estonia of using anonymous virtual currency wallets¹⁵⁸ for both storing funds of criminal origin and as intermediary addresses to direct funds into use through a centralized service provider after passing through a certain number of intermediary addresses (to conceal the original source of the funds). Both FATF and FinCen¹⁵⁹ have emphasized the risks associated with anonymous wallets. On one hand, it is the safest way for the user to manage their funds, but on the other hand, the requirements of the MLTFPA do not apply due to the absence of a centralized service provider. The use of anonymous wallets allows criminals to hide the ownership of wallets, which has also been seen in several criminal proceedings in Estonia.

For example, a recent case involved bitcoins earned from drug sales being moved in ways that did not use a central service provider for managing the virtual currency. The purpose of such virtual currency movements is to conceal the origin of the money by using anonymous virtual currency wallets, making it more difficult for law enforcement agencies to identify the origin and owners of the virtual currency.

Therefore, it is important that VASPs apply enhanced due diligence measures for clients whose transactions are related to anonymous virtual currency wallets.

6.4.4. Cyber threats

International blockchain software producers TRM Labs and Chainalysis confirm in their annual reports that crime facilitated through blockchain is becoming increasingly diverse and professional. There is a specialization in offering certain services, such as the current popular trend of purchasing so-called off-the-shelf software solutions that provide infrastructure for various types of crime (e.g., environments for exchanging funds suspected of money laundering, attack software, or malware).¹⁶⁰ This situation has also been identified in Estonia, and law enforcement agencies have paid attention to and disrupted the activities of such service providers¹⁶¹.

According to Chainalysis, 63% of the total volume of illegal transactions is facilitated through stablecoins, and this practice is also reflected in Estonian crime. This is a prevailing trend in the ecosystem; despite these trends, some forms of crypto crime, such as ransomware and dark web activities, are still dominated by bitcoin. However, according to the reports of Estonian VASPs, transactions with the most popular stablecoin, USDT, account for only 3%.

¹⁵⁸ Uhosted/non-custodial/self-custody wallets.

¹⁵⁹ Financial Crimes Enforcement Network.

¹⁶⁰ <https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem>

¹⁶¹ 1-24-6223, 20.11.2024.

In terms of cyber threats, Estonian VASPs have mostly been in the role of victims. They have been attacked, resulting in significant losses of virtual currency. In 2024, several attacks were directed against Estonian VASPs. In 2023, the attacks on AtomicWallet and CoinsPaid also gained international attention, with criminals seizing virtual currencies worth more than 150 million euros. Both attacks have been linked to the North Korean state-supported hacker group Lazarus Group.¹⁶²

According to the Estonian Information System Authority, the largest share of impactful cyber incidents in 2024 consisted of various phishing and scam websites (an increase of nearly 2.5 times in the number of incidents compared to the previous year). Additionally, investment scam websites were identified, where, after a temporary decline, various virtual currencies were again prominently represented alongside stocks.

6.4.5. Fraud

There continues to be a significant trend of various frauds, resulting in criminals obtaining virtual currencies in Estonia. For example, in 2023, a person was convicted in Finland for committing a cyberattack (exploiting a logic error in online games) against one of Estonia's largest virtual casino online gaming platforms, resulting in the fraudulent acquisition of virtual currencies worth nearly 1.3 million euros. The cybercriminal was convicted based on evidence collected in Estonia, and assets worth 1.5 million euros were confiscated.

One of the most notable fraud cases in recent years is the Hashflare case, where two Estonian individuals offered clients contracts that allowed them to obtain a share in HashFlare's mining operation, receiving a portion of the virtual currency produced. However, the company did not have the alleged virtual currency mining equipment, and when investors requested to withdraw their mining profits, HashFlare was unable to pay the promised mined funds. Between 2015 and 2019, people entered into contracts with this company worth 577 million dollars. At the time of the report, the individuals had pleaded guilty (reached a settlement) to conducting the fraud.¹⁶³

Additionally, a company and associated individuals have been suspected of investment fraud for providing false information to sell their created virtual currency, Dagcoin (created in 2018). According to the suspicion, false information was provided when selling the virtual currency. The price of Dagcoin depended on the number of its users – the more people who accepted Dagcoin as a means of payment, the higher the price. It is suspected that, to obtain investments, the price of Dagcoin and the number of its users were artificially increased, creating the public perception of a functioning and continuously value-growing virtual currency that could be used as a means of payment or to earn income from its storage. The proceedings were ongoing at the time of the report.

6.4.6. Drug-related crime

Drug-related crime in Estonia is closely linked to virtual currencies. Criminals use both closed Telegram groups and the dark web to sell drugs, where the buyer pays for the drugs in virtual currency. The trend is more towards drug sales moving from the dark web to closed Telegram groups. Several publicly known criminal proceedings confirm this, where drug-related crime has been associated with virtual currencies.¹⁶⁴ There have also been cases where criminals have tried to conceal the origin of assets obtained from drug crimes, resulting in the criminal being suspected of money laundering.¹⁶⁵

¹⁶² For more detailed information, you can read the report related to the risks of financing weapons of mass destruction.

¹⁶³ <https://www.justice.gov/opa/pr/two-estonian-nationals-plead-guilty-577m-cryptocurrency-fraud-scheme>

¹⁶⁴ RKKK 1-21-7128; HMK1-17-10573.

¹⁶⁵ <https://ekspress.delfi.ee/artikkel/120344625/pensionisammas-politseiaigendi-kaest-saadud-fentanuulirahaga-majandas-narkoari-ka-naine>

For Estonian law enforcement agencies, investigating money laundering crimes is challenging, and a prerequisite for a successful investigation is the existence of a predicate offense, which usually requires effective international cooperation. However, in the case of drug crimes committed in Estonia, the extended confiscation of assets obtained from the crime is applied, which has the same effect in essence but is significantly easier to prove than money laundering.

In summary, the main threat related to drug crime in Estonia is the use of virtual currencies as a means for criminal purposes. Virtual currencies are a convenient and anonymous means for criminals to legalize illicitly obtained proceeds.

6.4.7. Application of due diligence measures in correspondent relationships

VASPs are most vulnerable to money laundering and terrorist financing when servicing correspondent relationships, as due diligence measures are not applied at a sufficient level in such client relationships.

The MLTFPA defines correspondent relationships as relationships between financial institutions (including VASPs), including those in which the correspondent institution provides similar services to the respondent institution for serving its clients, and relationships established for conducting crypto asset transactions or transfers.

Providing correspondent services involves higher-than-usual money laundering and terrorist financing risks because:

- The correspondent institution usually does not have a business relationship with the ultimate beneficial clients and typically does not know their identity or the nature or purpose of the underlying transaction, which can make it difficult to identify suspicious transactions and reduce the ability to apply adequate due diligence measures to these transactions.
- Correspondent institutions generally do not apply due diligence measures directly to the ultimate beneficial clients themselves but rely on their clients, who may not effectively identify risky activities or their clients, i.e., the ultimate beneficial clients.
- Identifying the ultimate beneficial owners and the origin of the assets used in transactions is more complicated than usual.
- There is at least one additional link in the chain of asset movement, and transparency is reduced from the perspective of preventing money laundering and terrorist financing.

The FIU has identified correspondent relationships in the supervision of VASPs, but based on the collected data, only a few VASPs had previously defined such relationships as correspondent relationships. In 2023, only 2 VASPs informed FIU that they had established correspondent relationships with clients, but by the end of 2024, 16 VASPs had reported correspondent relationships. Correspondent relationships accounted for only 0.07% of all VASP clients in 2024, of which 40% were other VASPs and 60% were other financial institutions. Correspondent relationships accounted for a total of 7.34% of all service volumes in 2024.

In one case, the result of FIU's supervisory procedure revealed that one VASP had nearly 80% of its client relationships as correspondent relationships. The company had not identified or understood the nature and risk environment of correspondent relationships and, as a result, had not applied due diligence measures to clients or transactions. A similar case was identified in 2022 when Garantex Europe OÜ presented physical persons as clients, but the supervision revealed that they were representatives of legal entities who, in turn, provided services to their clients.¹⁶⁶

¹⁶⁶ <https://fiu.ee/uudised/garantex-europe-ou-kaotas-oiguse-pakkuda-virtuaalvaaringutega-seotud-teenuseid>

In correspondent relationships, the third party is often another VASP or other financial institution. In such services, the assets of the ultimate beneficial client are moved through the VASP without knowing the origin of the money and wealth. In the responses to the expert group's survey conducted during the risk assessment, most VASPs indicated that services related to correspondent relationships are more exposed to money laundering and terrorist financing risks and that they have established separate due diligence measures to mitigate these risks. However, there is a contradiction between the situations identified in the supervision and the responses of the VASPs. The contradiction indicates that **VASPs are not sufficiently aware of client relationships that are essentially correspondent relationships**. Service providers have not taken sufficient measures to identify whether the client is a person who provides services to their clients. This, in turn, increases the vulnerability of VASPs to money laundering, terrorist financing, and sanctions evasion, as VASPs are unable to apply adequate due diligence measures in such relationships. Therefore, it is justified that VASPs pay additional attention to identifying correspondent relationships and subsequently applying due diligence measures.

6.4.8. Correspondent relationships with high-risk areas

Statistics from the FIU confirm that only a few legal clients in offshore areas¹⁶⁷ generate significant turnover. At the end of 2024, legal entities made up only 0.5% of the total number of clients of Estonian VASPs, but their transaction volume was nearly 62% of all transactions. Most legal entities come from offshore areas, with which Estonian VASPs are likely to have correspondent relationships.

The risk is particularly high if a VASP has a correspondent relationship with companies located in high-risk countries¹⁶⁸ or offshore areas. Offshore or low-tax territories or countries are often associated with higher money laundering and terrorist financing risks because international assessments indicate that their risk management solutions are inadequate or these countries are used to obscure the data of beneficial owners.

The total volume of services provided to residents of countries with a higher risk level of terrorist financing among Estonian VASPs accounted for less than 1% of all services in 2024. The share of clients was less than 0.5%. Legal entities accounted for more than half (66%) of the turnover from high-risk countries and 12% of the clients. This indicates that the movement of virtual currencies related to high-risk countries is again more associated with legal entities, which in turn points to potential risks related to correspondent relationships.

Most cases of suspected terrorist financing originate primarily through correspondent relationships. Transactions with these connections usually do not occur within the Estonian jurisdiction, but individuals deposit funds through an Estonian VASP.

An illustrative example of the risk of correspondent relationships and terrorist financing is a case in 2023 where an 18-member network was identified that wanted to conduct transactions in virtual currencies through an Estonian VASP. In this situation, a correspondent relationship had been established with the Estonian VASP. Therefore, in terms of terrorist financing, Estonia is more in the transmission stage, similar to money laundering risks. While investigating the case, FIU and the ISS froze assets worth 8,205 euros. Several Estonian VASPs have also pointed out in their responses to the expert group's questionnaire that correspondent relationships are more exposed to terrorist financing risks compared to regular services.

¹⁶⁷ Low-Tax Territories or Countries.

¹⁶⁸ FIU, https://fiu.ee/sites/default/files/documents/2024-09/Lisa.%20K%C3%B5rgema%20terrorismi%20rahastamise%20riskiga%20riikide%20nimekiri_18.09.2024.pdf

6.4.9. Correspondent relationships and gambling organizers

Client relationships between VASPs and gambling operators are not considered correspondent relationships, even though the nature of ML and TF risks is similar (the end client, i.e., the gambling operator's client, uses the VASP's services). VASPs are not required to apply the due diligence measures stipulated in § 40 of the MLTFPA in relationships with gambling operators, even though the money laundering and terrorist financing risks in these client relationships are similar to those in correspondent services. The results of regular reporting by VASPs indicate that a very large volume of transactions by Estonian VASPs is likely related to gambling operators.

For example, in 2024, the service volume for virtual currency wallet services with clients from the offshore area of Curacao, associated with crypto casinos, accounted for 54%, and for transfer services (without changing the currency), it accounted for 31% of the total volume of the mentioned service. Across all services, the number of clients was less than 0.1%. Among the clients with higher turnovers in offshore areas were also the Isle of Man, Cyprus, Seychelles, British Virgin Islands, Vanuatu, etc. In several offshore areas, there were no individual clients at all. Based on supervisory procedures and other public information, many of these areas can be associated with gambling operators.

Risks of Estonian licensed VASPs are concentrated around crypto casinos. **The offshore areas mentioned in the previous section are associated with crypto casinos, where the quality of supervision is questionable.** According to the current requirements of the MLTFPA, VASPs are not obliged to identify who the client of the crypto casino is (the end client of the VASP's services), i.e., who deposits their virtual currencies into a virtual currency wallet opened with an Estonian VASP, owned by the crypto casino. By providing services to crypto casinos or related companies, VASPs also take on the risks associated with the clients of crypto casinos. This was highlighted in the EU-wide risk assessment (SNRA)¹⁶⁹ completed in 2022. According to international studies¹⁷⁰ and typologies, crypto casinos are increasingly involved in laundering funds obtained through various crimes and are more frequently used by organized criminals.

Having such clients significantly amplifies the risks for VASPs, as thousands or hundreds of thousands of subsequent clients may be hidden under the "account" of one legal entity client, whose identification and transaction monitoring are beyond the capabilities of the Estonian service provider, and the risks of money laundering or terrorist financing may materialize.

On one hand, the risks for Estonian licensed VASPs and gambling operators are high because the volume of services is so large, and VASPs are vulnerable because there is no legal obligation to apply due diligence measures similar to those for correspondent relationships in such business relationships. Therefore, it is appropriate, based on this risk assessment, that VASPs apply enhanced due diligence measures in client relationships with gambling operators.

Technology-Related Threats

In an ever-evolving world, criminals are increasingly seeking new solutions to use for money laundering, terrorist financing, or evading financial sanctions. The use of various new technologies brings forth risks that must be considered. In recent years, the adoption of artificial intelligence (AI) has significantly expanded, which, on one hand, creates many opportunities, but on the other hand, also brings many risks. One new threat is the use of deepfake technology, which can significantly complicate the implementation of anti-money laundering measures and pose additional risks to VASPs. Deepfake technology poses a serious threat to the

¹⁶⁹ https://www.fin.ee/sites/default/files/documents/2022-11/CELEX_52022SC0344_EN_TXT.pdf

¹⁷⁰ <https://fintrac-canafe.canada.ca/intel/operation/iso-osi-eng.pdf>, https://static.rusi.org/north-korean-activity-in-casino-gaming-industry_0.pdf

reliability of identity fraud¹⁷¹ and KYC¹⁷² processes. It can be used to create fake images of identity documents, which can be used to open bank accounts or virtual currency wallets. Additionally, AI-generated fake facial recognition videos can deceive biometric KYC systems, allowing criminals to hide their true identity. Deepfake voices can be used to manipulate phone-based KYC processes, jeopardizing the effectiveness of anti-money laundering and counter-terrorist financing measures. Furthermore, deepfake technology can be used to deceive companies and financial institutions. Fraudsters can create fake videos or audio recordings to impersonate company executives and convince employees to make unauthorized payments or share sensitive financial information.¹⁷³ **Therefore, it is crucial that VASPs, among others, implement effective preventive measures (including various technical solutions) to prevent their use for money laundering (reducing their vulnerability), terrorist financing, or evading financial sanctions using new technologies. VASPs must monitor the ability of KYC service providers to prevent account creation using deepfake technology and generally invest more in mitigating fraud-related risks.**

In 2024, the top ten themes of suspicious transaction reports related to money laundering and terrorist financing submitted by Estonian VASPs included reports related to identity theft and forged documents. This confirms that the risk exists in the VASP sector. Although most VASPs stated in their responses to the NRA expert group's questionnaire that they have systems to detect the risks of deepfake technology, global trends indicate that the risk level in the sector is rather increasing, which therefore requires additional risk mitigation.

Phishing conducted by criminals is rapidly reaching new heights thanks to the development of artificial intelligence. Phishing involves manipulating people to fraudulently gain access to confidential information, systems, or even physical locations. Instead of trying to enter computer systems, people are manipulated – their trust or behavior driven by ignorance and fear is used to gain access to systems. For example, phishing techniques were used to steal virtual currencies from an Estonian VASP in 2023. Account takeover attacks on VASPs or their clients are becoming more common, and **two-factor authentication is no longer sufficient protection for logging in or confirming transactions.**

One possible solution to mitigate the risks described above could be the development of digital identity solutions to prevent identity theft. The requirements set out in the current legal norms focus on the creation of identity by and at the service provider, which means that one person has multiple identities, each of which is a separate target for attack. The minimum requirements for remote identification of individuals should be significantly strengthened, and the preference should be given to reusable identity solutions based on personal digital certificates, created using data read and verified from the biometric identity document chip (not data obtained by photographing the document). This alone would reduce the possibilities where a business relationship is established with a client whose document is actually created using various technological solutions. Cooperation between the public sector, VASPs, and service providers offering such solutions is crucial in this regard.

6.4.10. Operating without a license

Many VASPs that have lost their licenses in Estonia have applied for licenses in Lithuania. The number of VASP licenses in Lithuania increased from 8 in 2020 to 850 by the end of 2022. Several Estonian corporate service providers also advertise VASP licensing services in Lithuania on their websites, indicating that Estonian service providers who lost their licenses in Estonia have moved there.

¹⁷¹ [Report: Account Takeover Attacks Grew Over 800% against](#)

¹⁷² Know Your Customer – The purpose of the process is to understand who this specific client is, what service they want, and for what reason, i.e., whether the client's request aligns with their actual activities, capabilities, and needs, as well as the client's knowledge and understanding of the specifics and nature of their business activities, etc.

¹⁷³ Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks. <https://www.fsisac.com/hubfs/Knowledge/AI/DeepfakesInTheFinancialSector-UnderstandingTheThreatsManagingTheRisks.pdf>

There have been isolated cases in Estonia where VASPs known to have lost their licenses have continued to offer services despite this. For example, in 2024, there was a court case that revealed that Garantex Europe OÜ, which had lost its VASP license in Estonia (now a deleted legal entity from the business register), was offering virtual currency services without the appropriate license. According to the court ruling, the board members of Garantex Europe OÜ were found guilty of helping the company continue providing services after relinquishing its virtual currency service license, but now covertly and illegally. The state and authorities have responded to unlicensed activities according to the increased risks. In the future, **heightened attention should be directed towards unlicensed activities, and measures should be developed to methodically mitigate this risk across the sector**. Especially considering that in the future, VASPs that do not apply for a license from the FSA will also lose the license issued by the FIU, which may create a situation where VASPs continue to operate illegally without a license.

6.5. Assessments

The level of money laundering threat in the sector is **above average** for both virtual currencies and virtual currency service providers. The main risk is the use of virtual currencies for criminal purposes, rather than risks arising from Estonian VASPs.

The level of vulnerability to money laundering in the sector is **above average** for both virtual currencies and VASPs.

The residual risk level in the VASP sector is **medium**.

The risks in the VASP sector have decreased compared to previous periods – reports and foreign inquiries about market participants are on a downward trend. There are fewer market participants, and cooperation and understanding of risks have improved. Several legislative changes have contributed to the improvement of the situation. Additionally, mandatory reporting for VASPs has been established since 2024.

The risks have not completely disappeared, as transaction volumes are still large, transactions are global (often related to offshore areas), and to some extent anonymous. The highest risks by service are overwhelmingly associated with the most popular virtual currency wallet services, virtual currency exchange services, and transfer services. To reduce the level of vulnerability and better understand the risks, it is necessary for VASPs to continuously enhance their knowledge of money laundering and terrorist financing threats in cooperation with the public sector.

Heightened attention should be paid to the risks of correspondent relationships and other similar business relationships, especially in connection with so-called **crypto casinos**, because by providing services to crypto casinos or related companies, virtual currency service providers also take on the risks associated with the clients of crypto casinos.

7. ML Threats and Vulnerabilities of Legal Entities

7.1. Description of the Methodology

To assess legal entities, a new World Bank assessment module was used, focusing on evaluating the possibilities of exploiting legal entities for money laundering. The module analyzed the possibilities of creating legal entities, their number and behavior patterns, their connections with non-residents and foreign countries, the existing legal framework, the effectiveness of supervision, and the transparency of data published in registers. The availability and reliability of beneficial ownership data were also assessed, and risk typologies in which legal entities were used to commit money laundering offenses were examined.

Table 74. Module used for assessing the exploitation of legal entities for money laundering

Field	Assessment module
Legal entities	Legal Persons and Arrangements ML Risk Assessment Tool (2022)

In assessing risks, the statistics of court decisions on money laundering cases, crimes committed with the artificial involvement of legal entities, and the extent of criminal proceeds obtained through them were taken into account. Additionally, risk typologies that emerged in international information exchange and reports received by the FIU involving legal entities registered in Estonia were considered.

In assessing vulnerabilities, the quality and reliability of data published in the Business register and the beneficial ownership register were considered, as well as the measures for verifying the accuracy of this data. The risk awareness of market participants, particularly corporate service providers, and the quality of due diligence measures, access to data by market participants, and their ability to verify data and identify individuals were also taken into account. Furthermore, the effectiveness of local supervision and international information exchange was assessed.

Quantitative data from the Business register, the beneficial ownership register, statistics from supervisory authorities, and international information exchange data were used in the risk assessment, as well as qualitative expert assessments and cases collected by the working group where legal entities registered in Estonia were used to commit crimes (including money laundering).

The preliminary analysis also included: general partnerships, limited partnerships, foundations, European companies (SE), European economic interest groupings (EEIG), European cooperatives (SCE), branches of foreign companies in Estonia, and apartment associations.

7.2. Risks of Legal Entities

The conclusions presented in this chapter focus on four legal forms of legal entities: private limited company (OÜ), public limited company (AS), non-profit association (MTÜ), and cooperative (TuÜ), which together constitute 83% of all legal entities¹⁷⁴ in Estonia. These legal forms dominate identified money laundering schemes and suspicious information, are the most registered in the Business register, and have the largest volume of transactions and assets (Table 32).¹⁷⁵

Almost all forms¹⁷⁶ of legal entities in Estonia were included in the preliminary analysis, but for others, the involvement in money laundering schemes was either very minimal or non-existent, and their overall number and asset volume were very small. As a result of the analysis, the residual risk level of private limited companies was assessed to be **above average**, while the residual risk level of public limited companies, non-profit associations, and cooperatives was assessed to be **lower than average** (see Table 75).¹⁷⁷

Among other forms of legal entities, private limited companies have the highest residual risk level for money laundering in Estonia, as cases and suspicious information indicate that private limited companies are clearly the most common legal form used for money laundering. Additionally, the total sales revenue of private limited companies is the highest. Establishing private limited companies is relatively easy, and the liability of a natural person for the activities of a legal entity is limited.

Table 75. Legal forms of legal entities in Estonia with the highest risk levels for money laundering

By 31.12.2024	In total	Connection to foreigners	Share of non-active ¹⁷⁸	Turnover	Asset volume	Residual risk
Private ltd or OÜ	262,809	26%	48%	60.8 mld	97.3 mld	Above average
Public ltd co or AS	2,164	45%	9%	34.3 mld	112.8 mld	Below average
NPO or MTÜ	22,657	12%	8%	1.0 mld	0.8 mld	Below average
Cooperative or TuÜ	1,529	28%	84%	2.0 mld	0.9 mld	Below average

Source: Business Register

The use of legal entities in money laundering is widespread because it allows for the concealment of the real individuals behind the money laundering scheme and disperses the liability of a natural person. According to the NRA working group, the involvement of a legal entity in money laundering-related criminal proceedings and court decisions is not an independent threat but reflects the nature of a society with low cash usage and electronic operations. Due to its small size, Estonia primarily serves as a transit country in money laundering schemes, which also necessitates the involvement of legal entities in the scheme. Considering

¹⁷⁴ As of the end of 2024, a total of 348,289 legal entities are registered in the Business register.

¹⁷⁵ The table presents the latest known data for the period under review in the report, i.e., the first three columns contain data as of the end of 2024, and the last two columns contain data from the annual reports submitted for 2023.

¹⁷⁶ The preliminary analysis also included: general partnerships, limited partnerships, foundations, European companies (SE), European economic interest groupings (EEIG), European cooperatives (SCE), branches of foreign companies in Estonia, and apartment associations.

¹⁷⁷ The residual risk assessment for public limited companies was closer to the average level, while the assessment for cooperatives was closer to the “very low” level.

¹⁷⁸ To distinguish between active and inactive legal entities, the methodology of the Statistics Estonia is used, according to which the main criteria for differentiation are sales revenue, salaried employees, investments made, and other signs of economic activity from various sources.

the role of legal entities in Estonia's e-society, the assessments of the threats (higher than average) and vulnerabilities (average) of legal entities, and the dominance of the private limited company form among legal entities suspected of money laundering, the overall **residual risk** level of exploiting legal entities for money laundering in Estonia is **medium**.

7.3. Attractiveness of Estonian Companies

In Estonia, establishing a legal entity is simple and inexpensive for both Estonian citizens and foreigners, and the legal framework for establishment is similar for both. Private limited companies, general partnerships, limited partnerships, and non-profit associations can be established either through the e-Business Register or with the help of a notary. If a person does not have a digital ID, they must go to a notary to establish a company or acquire shares in a company (it is possible to use powers of attorney, including the services of company service providers). To establish a public limited company, foundation, cooperative, apartment association, European company, European economic interest grouping, or European cooperative, one must contact a notary. According to the commercial register, approximately 87% of legal entities are established annually through the e-Business Register.

The attractiveness of establishing a company in Estonia is further enhanced by the fact that, since 2023, it has been possible to establish a private limited company without a share capital contribution (private limited companies can be established with a share capital of just one cent). Moreover, it is not necessarily required to open a payment account in Estonia for the company's activities. The ease of establishment allows for the creation of new private limited companies as desired, and problematic private limited companies can essentially be abandoned. To reduce the number of inactive companies, a significant number of legal entities that failed to submit annual reports were deleted from the commercial register in 2024.

As of February 1, 2023, the residency requirement for the management board was abolished for all forms of legal entities. The residency of shareholders, members, and participants is not regulated by corporate law. A private limited company is a classic limited liability company, meaning that shareholders generally do not bear responsibility¹⁷⁹ for the company's obligations.

The Estonian legal system does not recognize the service of a nominee director. All members of the management board must always act in the best interests of the legal entity as a whole, and all members of the management board are responsible for the activities of the legal entity, including criminal liability. **It is not possible to use bearer shares in Estonia** (prohibited since January 1, 2002). There is no possibility to operate in special zones (such as customs zones), and it is not possible to register any separate legal entity form for this purpose in Estonia. Under Estonian law, it is also not possible to establish trusts. Since 2022, information about trustees operating in Estonia and trusts established in other countries must be disclosed¹⁸⁰ in the e-Business Register information system.

The attractiveness of Estonian companies is further enhanced by the significantly strong protection of property rights. For example, unlike many EU countries, property is not confiscated in criminal proceedings without a conviction. Additionally, there is no effective and widely used administrative confiscation measure in Estonia. Section 57(7) of the MLTFPA allows for the transfer of property suspected of being involved in

¹⁷⁹ According to § 167¹ (1) of the Commercial Code, a person who, by using their influence over a private limited company, has influenced a member of the management board, supervisory board, or a procurator to act to the detriment of the private limited company, must compensate the company for the damage caused. Additionally, in the event of insolvency, a temporary bankruptcy trustee has the right to demand payment and reimbursement of expenses from the shareholders of the private limited company up to 2500 euros if the company's share capital is less than 2500 euros.

¹⁸⁰ According to MLTFPA § 77 (3³), (3⁴) and (4²).

money laundering to the state, but only if the owner of the property or the beneficial owner of the property in the account is unknown. The guarantees for the protection of property rights provided by the Estonian state for the seizure of property to ensure confiscation are greater than in many other EU countries. Seized property is generally not alienated without the owner's consent but is kept in state custody, which is not always the best solution for preserving the value of the property and the most efficient use of taxpayer money. There is also no possibility to use seized property for social or public purposes (for example, in France, seized vehicles are used by local investigative authorities).

One of the arguments for establishing a company in Estonia is the favorable tax environment (e.g., there is no corporate income tax on undistributed profits). Estonia's attractiveness is also demonstrated by the fact that Estonia has been ranked first in the International Tax Competitiveness Index¹⁸¹ for more than ten years in a row, as Estonia has a very convenient and mostly automated tax system. **Although tax competition is high, Estonia is not considered a tax haven**, as shown by the Corporate Tax Haven Index¹⁸², where Estonia ranked 34th in 2023 (ahead of Estonia were, for example, Finland and Sweden). Aspects that reduce attractiveness include the small size of the Estonian market and relatively high input costs, including labor taxes and energy prices.

7.4. Threats of Money Laundering with Legal Entities in Estonia

The overall threat level of money laundering with legal entities is above average. It is very difficult to commit money laundering that poses a threat to the economy in Estonia without involving a legal entity.

This is illustrated by the fact that all criminal cases investigated between 2020 and 2024 included a legal entity either as a channel or perpetrator of money laundering. It is important to note that the total number of money laundering criminal proceedings is extremely small¹⁸³ compared to other types of crime. However, the economic damage identified in money laundering cases that have resulted in convictions has been significantly greater compared to other types of crime (on average 780,000 euros in money laundering cases, plus cases involving over a billion euros).

Money laundering schemes involving Estonia often use a network of companies and individuals spread across multiple countries, with the actual beneficiaries possibly located in countries such as Ukraine, Russia, and other third countries. However, companies registered in other European Economic Area countries and the accounts of credit and payment institutions registered in those countries are most often directly involved with Estonia. **The fact that legal entities are often used in international money laundering schemes raises the overall risk level above average.** For example, 80-90% of outgoing legal assistance requests from Estonia at the prosecutor's level are related to legal entities, and legal entities also dominate incoming legal assistance requests. International cooperation is time-consuming even with jurisdictions where cooperation works. Moreover, the European Investigation Order (EIO) does not function effectively, making proceedings slow and increasing the risk of expiration.

The main form of legal entity used for money laundering in Estonia is **the private limited company, and similar limited liability private business forms from other European Economic Area countries**. Among the nine foreign legal entities¹⁸⁴ analyzed, two stood out somewhat more than the others, although the differences are not

¹⁸¹ <https://taxfoundation.org/research/all/global/2024-international-tax-competitiveness-index/>

¹⁸² <https://cthi.taxjustice.net/full-list>

¹⁸³ Between 2020 and 2024, an average of 25,000–28,000 crimes were registered annually in Estonia, but there were only 74 criminal proceedings related to money laundering over the five-year period. <https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2024/kriminaalmenetluse-statistika>

¹⁸⁴ Finnish OY, Latvian SIA, Lithuanian UAB, German GmbH, Spanish SL, Cypriot LTD, Maltese LTD, UK LTD, Dutch BV. The selection was based on the FIU's suspicious information, criminal proceedings, and court decisions.

very large. The Estonian business environment is equally open to all European Economic Area countries, but based on the risk assessment, the **Lithuanian UAB and the UK LTD** stood out somewhat from the others. The Lithuanian UAB stood out due to its more frequent involvement in money laundering schemes related to Estonia. For the UK LTD, the greater risk compared to others is the poorer availability of information about the people associated with the company, including the actual beneficiaries.

7.4.1. ML threats and trends identified from court cases

In a society with low cash usage like Estonia, it is difficult to commit money laundering that poses a threat to the economy without the involvement of a legal entity, either as a channel (e.g., using a payment intermediary) or as a perpetrator. Between 2020 and 2024, all criminal proceedings involved a legal entity in some form of money laundering. Even if the perpetrator of money laundering is not a legal entity, legal entities are involved in the money laundering scheme, for example, through a payment intermediary bank.

The high number of suspicious transaction reports and referrals made by the FIU compared to the small number of criminal proceedings may indicate that there are more problematic cases than the state supervisory authorities can handle.

One typology identified from court cases is the opening of bank accounts in the name of Estonian companies, into which money obtained from predicate offenses committed abroad is transferred to conceal its illegal origin and integrate it into the legal economy. The most common example was the movement of funds obtained through business fraud¹⁸⁵ committed abroad through the bank accounts of Estonian companies in Estonia.

A typology of money laundering that emerged between 2020 and 2024 was the use of informal virtual currency exchange points in Estonia and neighboring countries, where the person organizing the money laundering received cash and immediately made a payout in the chosen cryptocurrency to the money launderer's wallet. This method was used, for example, by international organized crime with money obtained from fraud. Individuals often concealed their profits and transactions through the activities of legal entities or directed payouts to legal entities. Additionally, during this period, there were two cases where virtual currency exchange platforms were created as new legal entities with registrations in the UK and Lithuania, but were managed from Estonia to further conceal their activities.

A trend in predicate offenses for money laundering during the period was the violation of international sanctions. Specifically, a new phenomenon emerged where there was a need to conceal the criminal proceeds obtained from the delivery of sanctioned goods to Russia and Belarus or to transfer funds from those areas. There was also one case where an Estonian legal entity knowingly provided consulting services prohibited by sanctions to Russian companies, and the profits from this were channeled to Europe through a shell company in Georgia.

7.4.2. Threats and trends from reports submitted to the FIU

One of the most common practices involving legal entities in money laundering schemes related to Estonia is the dispersion of activities across different jurisdictions¹⁸⁶. This is particularly evident in the suspicious information submitted to the FIU, but there are also examples from criminal proceedings. Among others, this practice is used by professional money laundering service providers (see Case 1).

¹⁸⁵ BEC – business e-mail compromise

¹⁸⁶ Multi-jurisdiction splitting

CASE 1: Money Laundering by a Ukrainian PEP through Estonian Companies

The money that arrived in Estonia was transferred through various accounts of Estonian and foreign companies controlled by the individuals who created the scheme. To create an appearance of legitimate transactions, various contracts were drawn up to create fictitious debt relationships, which allowed the true origin of the money to be concealed. According to the collected evidence, a large portion of the money eventually returned to the high-ranking Ukrainian state official and former Minister of Health, Maksym Volodymyr Stepanov, or individuals closely associated with him.¹⁸⁷

The information collected and analyzed by the FIU also includes references to the use of **shell companies** and possible straw men for money laundering. The Estonian legal framework does not recognize the service of a nominee director, but in practice, Estonian companies are used in money laundering schemes, which are created either in the name of a conscious straw director or individuals who have fallen victim to identity theft or have knowingly sold their data. This means that in such cases, the official member of the management board of the legal entity does not have actual control over the activities of the legal entity (see case 2), although they are responsible for the activities of the legal entity. Additionally, there are examples where de facto nominee director services were provided by corporate service providers (including advertising this on their website). There have also been cases in the legal profession where the bar association has been notified that a lawyer is on the governing body instead of the client, but then the lawyer changes their position and mentions that it is their own company. However, this ends the supervision of the bar association, and no further actions are taken.

CASE 2: Exploitation of Companies Registered in the Names of Straw Men

The information analyzed by the FIU indicates the activity pattern of an international money laundering network. As a result of possible identity theft, numerous Estonian companies were established in the names of Estonian citizens, and either Estonian bank accounts or payment or e-money institution accounts in other EU countries were opened for them. These companies are suspected of being used to collect and launder criminal proceeds obtained from fraud. The companies were established through an Estonian company service provider (CSP).

Internationally, **it is common to use legal entities, including shell companies, to commit tax fraud and money laundering**. By using shell companies, criminal activities are given a seemingly legal appearance. In Estonia, there is a significant number of inactive companies¹⁸⁸ that have no real activity in Estonia but may be used to commit crimes in foreign countries (see the case in the e-residents chapter).

¹⁸⁷ <https://www.aripaev.ee/uudised/2025/02/04/prokuratuur-suudistab-kolme-eestlast-ukraina-eksministri-miljonite-rahapesus>

¹⁸⁸ By September 2024, 12% of the companies that were registered in the Business register as of April 30, 2023, had been deleted due to inactivity. Of those companies that had a connection with a foreigner, a total of 17%, or nearly one in five, were deleted. <https://fiu.ee/sites/default/files/documents/2024-10/V%C3%A4lismaalase%20seosega%20ettev%C3%B5tted%20poolteist%20aastat%20hiljem.pdf>

In 2022, the FIU, in cooperation with foreign financial intelligence units, identified **a criminal behavior pattern involving the misuse of Estonian companies with VAT registration numbers (KMKR)**.¹⁸⁹ This pattern is characterized by the involvement of predominantly foreign individuals, including e-residents.

1. A legal entity is established in Estonia, with the founder being either a CSP or a foreign individual. If the company is established by a CSP, a foreign individual is registered as the shareholder or member of the management board.
2. A VAT registration number is applied for the company. If the founder is a CSP, the VAT registration number is applied for before the change of shareholder and member of the management board.
3. The company conducts transactions mainly between payment accounts located abroad. Transactions can occur between the company's own accounts or with the accounts of other parties. The company may or may not have a bank account in Estonia.
4. The company has no declared activity in Estonia (e.g., no national taxes are declared, no turnover, and no employees) or the activity is minimal.
5. The activity pattern is illustrated by two schemes, which consistently involve an Estonian legal entity with a VAT registration number, a foreign shareholder and member of the management board, and transactions between accounts located abroad. In all described situations, the explanations of the shareholder and member of the management board regarding the transactions are difficult to verify, and the origin of the funds is unclear.

Since Russia launched its full-scale war of aggression against Ukraine in 2022, **the use of Estonian legal entities associated with Russian and Belarusian individuals to evade international sanctions has increased**.¹⁹⁰ The FIU is aware of cases where Estonian legal entities are used to make goods (i.e., economic resources) available to entities subject to financial sanctions. In these cases, the predicate offense for money laundering may be a violation of financial or trade sanctions. The typology report describes schemes where indicators include anomalies in economic indicators and activities, as well as connections to Russia and Belarus, such as through indirect ownership, contact information, etc.

The movement of goods and the structure of transactions are usually complex, and many legal entities, accounts, etc., from various jurisdictions may be involved in the transactions. In a very simplified form, the scheme can be structured as follows:

1. An Estonian legal entity purchases goods in a sanctioned sector from a foreign company.
2. The goods are then sold to a buyer in a Russia-friendly country, who in turn sells them to a Russian or Belarusian party. The goods may not necessarily pass through Estonia.
3. The funds are received, for example, in the account of the Estonian company, which may be located in Estonia or abroad.

Although Estonia is primarily a transit country for money laundering, there are also examples where the predicate offense for money laundering is committed in Estonia (see Case 3) or where Estonian citizens involved in the predicate offense integrate the criminal proceeds into Estonia (see Case 4).

¹⁸⁹ FIU Typology Report 1TT202212. <https://fiu.ee/sites/default/files/documents/2022-12/T%C3%BCpologiateade%201TT202212.pdf>

¹⁹⁰ FIU Typology Report 7TT202401. https://fiu.ee/sites/default/files/documents/2024-01/T%C3%BCpologiateade%207TT202401_1.pdf

CASE 3: Embezzlement of NPO Assets and Money Laundering through Private Limited Companies (OÜ)

An NGO received over 100,000 euros in grants from the Estonian state over several years. The funds were transferred in round sums to companies with various business activities. These companies exhibited characteristics of shell companies and had a suspicious background, being associated with criminal histories and interconnected individuals. The companies were also linked to the NGO's board member and the actual beneficiary's spouse. It is suspected that the embezzled assets were layered through private limited companies with shell company characteristics, with the same individuals on their boards.

CASE 4:

Two Estonian individuals were suspected of creating a company operating as a **Ponzi scheme** and causing damage amounting to over half a billion dollars. They invited people to invest in cryptocurrency mining company A, but in reality, they did not use the funds for developing the cryptocurrency mining operation but for their own purposes. The proceeds from the fraud were used to purchase real estate, luxury vehicles, and investments (including cryptocurrency purchases). The individuals were arrested in Estonia but were later extradited to the USA for trial, where they reached an agreement with the US authorities. Although the indictment in the USA did not specifically charge them with money laundering, the text of the indictment still accused them of activities that would be considered money laundering under Estonian criminal law – including acts of concealing criminal proceeds. The factual description of the offense also includes that the proceeds from the so-called cryptocurrency mining company A were not directed to the victims but to individuals and companies under the control of the accused, who in turn purchased real estate, vehicles, and jewelry in Estonia and elsewhere.

7.5. Vulnerabilities of Legal Entities

The vulnerability level of Estonian legal entities is medium. The main vulnerabilities in the exploitation of Estonian legal entities for money laundering are **the weak due diligence measures of so-called gatekeepers** and **the inadequacy of the beneficial ownership register (TEKSA) data**. Gatekeepers refer to professions whose services directly influence whether money laundering is facilitated or prevented (company service providers, lawyers, other legal advisors, notaries, accountants, auditors). Therefore, corporate service providers play a significant role in the vulnerabilities of legal entities, as they can create or control companies that may be used to conceal the ownership and movement of illegal funds and to evade sanctions.

7.5.1. Weak due diligence measures of gatekeepers

The vulnerability level of legal entities is directly influenced by the quality of due diligence measures implemented by market participants. During the period under review, credit institutions generally did not have problems with the application of due diligence measures, but the reporting activity (including quality) and **the implementation of due diligence measures by gatekeepers were still unsatisfactory as of the end of 2024**. The problems are particularly significant with company service providers (CSPs), who play an important role in the risks of legal entities. CSP representatives consider their risks to be rather low and their due diligence measures to be at a good level¹⁹¹. CSP representatives have pointed out that **their primary interest is to inform the client of an incorrect transaction and reverse the transaction if necessary, rather than first notifying the FIU**. However, the reporting activity of CSPs as obligated persons under the MLTFPA has been **consistently unsatisfactory** from 2020 to 2024.

¹⁹¹ Interview with CSP Representatives; Results of NRA Working Group Surveys.

The number of reports submitted by CSPs ranged between 9 and 46 from 2020 to 2024, and only 4% of CSPs submitted reports, which is too small a number considering¹⁹² the size and composition of CSPs' clients. According to the FIU's supervision, **the application of enhanced due diligence measures by CSPs is weak, and Estonian CSPs continue to be exploited for money laundering and related crimes.** From 2020 to 2024, the FIU focused increased attention on controlling the CSP sector and helped raise awareness in the sector through training (including training for CSPs), notices, and typology reports (see the CSP subchapter for more details).

The FIU receives over 10,000 reports annually, but the number of reports submitted by gatekeepers fluctuated between 280 and 390 from 2020 to 2024, constituting only 3% of all reports submitted to the FIU in 2024 (see the "Professional" row in Table 76).

Table 76. Distribution of reports submitted to the FIU by reporting groups in 2024

Reporter groups	Total	Total (%)	ML	ML (%)	TFR	TFR (%)	ISR	ISR (%)	CTR	CTR (%)
Credit institutions	5,351	39%	4,878	47%	57	33%	416	70%		
VASPs	4,158	30%	4,006	39%	59	34%	93	16%		
Financial institutions	1,965	14%	981	9%	44	25%	24	4%	916	36%
Gambling operators	1,358	10%	96	1%	1	1%			1,261	50%
Professional (law, audit, etc)	390	3%	166	2%	12	7%	18	3%	194	8%
Other private sector entrepreneurs	199	1%	83	1%			9	2%	107	4%
Government agencies	119	1%	67	1%	1	1%	24	4%	27	1%
Not an obliged entity	70	1%	61	1%			4	1%	5	0%
Foreign authorities and individuals	33	0%	28	0%			5	1%		
TOTAL	13,643	100%	10,366	100%	174	100%	593	100%	2,510	100%

Source: FIU

Similar to CSPs, the overall reporting activity of other gatekeepers is also insufficient, indicating that **service providers may still fail to identify suspicious situations, do not correctly apply the know-your-customer principle, or deliberately fail to fulfill their reporting obligations.** Considering that there are about a thousand members of the bar association in Estonia, roughly the same number of other legal advisors, and over 8,000 accounting and tax advisory firms, **the reporting activity of representatives of these core activities is questionably low** (see Table 76). Therefore, one of the main vulnerabilities in the exploitation of Estonian legal entities is the fact that **Estonian CSPs and other individuals fulfilling the gatekeeper function still do not understand the importance of their role as enablers or preventers in the fight against money laundering and terrorist financing** (see the non-financial sector chapter for more details).

It is also important to note that of the already few reports submitted by gatekeepers, only 50% are suspicious transaction reports, while the remaining half are threshold-based cash transaction reports (CTR). The proportion of CTRs is particularly high (90%) among reports submitted by auditors (see Table 77). The submission of threshold-based reports does not indicate the substantive functioning of gatekeepers' due diligence measures, but rather that they are aware of a specific reporting requirement.

¹⁹² According to studies published by the FIU in 2024, more than one-fifth of Estonian companies are associated with foreign individuals, and for at least a quarter of these, the nature of their activities is unknown. Corporate service providers offer various services to a significant portion of these companies.

Table 77. Reports Submitted to the FIU by Professionals by Main Activity Areas in 2024

Field of the activity	UTR	UAR	STR	ISR	CTR	TFR	TOTAL	CTR %
Notaries	48	10	22	9	77	7	173	45%
Auditors	5	1	3	3	108		120	90%
TCSPs	5	16	19	2		4	46	0%
Accountants	8	8	7	1	9	1	34	26%
Attorneys (members of Bar Association)	3	1	3	1			8	0%
Other legal advisors			1		2			0%
Bankruptcy trustees		1	1				2	0%
Bar association board								0%
Financial and tax advisors	1						1	0%
Bailiffs								0%
TOTAL	70	38	58	18	194	12	390	50%

Source: FIU

7.5.2. Issues with the BO register

There are three main interrelated issues with the BO or TEKSA register:

1. The information in TEKSA is not complete and not always accurate.
2. The registrar does not verify the accuracy of the information.
3. No one has been actually punished for knowingly providing incomplete or false information.

When registering a company in Estonia through electronic channels, information about the beneficial owners must be provided, but its accuracy is not verified. Although there is a system for submitting discrepancy reports in TEKSA, it can only be used (for a fee) by market participants. Additionally, a company for which a discrepancy report is made can knowingly correct the submitted false information. Furthermore, as of December 31, 2024, about 5% of private limited companies and public limited companies have not indicated their beneficial owners.

For a person viewing information about a legal entity in the Estonian commercial register, the same view displays information about the company's management body and contact person, as well as annual reports and beneficial owner information. The user does not understand that the information displayed for the same company in the same view comes from two different registers, which are under different ministries and for which false information may be punished with different fines.

According to § 95 of the MLTFPA, failure to provide information about the beneficial owner or knowingly providing false information is a **misdemeanor**, for which a shareholder, member, or partner of a private legal entity can be punished. However, the act or omission is only a misdemeanor if, as a result of the incorrect information, the obligated person is unable to fulfill the due diligence measure provided for in § 20 (3) of the MLTFPA (i.e., to identify the beneficial owner). A natural person can be fined up to 2,400 euros and a legal person up to 400,000 euros. **However, the sanction for providing false information to TEKSA has never been applied.**

Providing false information to the commercial register is a **crime** (§ 281 of the Penal Code), for which a natural person can be punished with up to 2 years of imprisonment and a legal person with a fine of up to 40,000,000 euros (i.e., the fine is up to a **hundred times higher** compared to providing false information to TEKSA). Although punishment for providing false information to the commercial register is not common, it has been done, unlike for providing false information to TEKSA.

7.5.3. Factors reducing vulnerability level

The **main factors that reduce the vulnerability level of legal entities** are:

1. Free access to information in the commercial register and TEKSA.
2. The absence of nominee director services¹⁹³ and bearer shares in the Estonian legal system.

In Estonia, there are examples where companies led by straw men are used in criminal activities, but the fact that Estonian legislation does not recognize nominee director services and bearer shares reduces the level of vulnerability. The versatility of the commercial register and unrestricted access to it also play a significant role in reducing vulnerability levels. Although the partial poor quality of information in the TEKSA register increases vulnerability levels, free access to the beneficial ownership register is a factor that reduces the overall level of vulnerability. **Combined** with the **absence** of bearer shares and nominee director services in the Estonian legal system, the freely accessible commercial register and TEKSA databases are better than average mitigation measures for detecting opaque structures. This is also confirmed by the prosecutor's assessment¹⁹⁴ and the FIU's study on foreigners¹⁹⁵, which indicate that complex and multi-layered company ownership structures are rarely used for money laundering in Estonia.

Additionally, the generally high level of due diligence measures implemented by Estonian credit institutions and the high level of domestic and international cooperation by Estonian authorities further reduce the vulnerability levels of legal entities. Anti-money laundering cooperation with other EU member states is the most seamless.

Looking ahead, it is important to emphasize that if access to the commercial register and TEKSA decreases due to stricter implementation of domestic data protection laws and changing EU regulations (e.g., the AML Directive and its sixth legislative package), but other circumstances remain the same, the vulnerability level of legal entities will rise above average.

RECOMMENDATIONS:

- **Gatekeepers must start applying due diligence measures more effectively.** From the perspective of exploiting legal entities, they are crucial service providers whose actions directly influence whether money laundering is facilitated or prevented.
 - If the accessibility of data in the Estonian commercial register and TEKSA decreases due to the application of data protection rules and changes in EU regulations, the overall vulnerability of legal entities to money laundering risks will increase, making the due diligence measures of gatekeepers even more important.
 - This, in turn, would require greater attention from supervisory authorities to the activities of gatekeepers.
- **The reporting activity and quality of gatekeepers must improve.** The current reporting activity and quality of gatekeepers do not correspond to the number of service providers, the volume of assets in the sector, and the clientele.
- **It is recommended that obligated persons** notify the commercial register keeper **and** the FIU or the FSA¹⁹⁶ if they become aware of a suspicion that the beneficial ownership information is not accurate.

¹⁹³ <https://www.fiu.ee/uudised/osa-ariuhinguteenuse-pakkujaid-vahendavad-estri-arikeskkonna-labipaistvust>

¹⁹⁴ Working group interview with Prosecutor's Office representatives.

¹⁹⁵ <https://fiu.ee/valismaalased-estri-ettevotetes/valismaalastega-seotud-ettevotete-tunnusjooned> p. 21.

¹⁹⁶ MLTFPA § 97 (1). The extrajudicial proceedings for misdemeanors provided for in this chapter are conducted by the FIU and the FSA.

8. ML Risks of E-residency Program

The residual money laundering risk level of the e-residency program is medium. The main money laundering risk associated with e-residency is the exploitation of companies established in Estonia in other countries. To mitigate these risks, several measures were taken between 2020 and 2024, the most important of which are the strengthening of pre-, post-, and background checks, and the focus on target countries with which Estonia has effective professional cooperation. However, there remains a risk that significant economic damage could be caused by international criminal schemes involving only one or two e-residents, which could result in reputational damage to the entire e-residency program.

8.1. Description of the Methodology

There is no separate assessment module created for evaluating the risks of the e-residency program. Partially, the case-based worksheet “Step 2C Case Studies” of the legal entities assessment module was used. The risk assessment was based on statistics related to companies associated with e-residents and data related to money laundering cases from the databases of the FIU, the PBGB, the TCB, and the Prosecutor’s Office.

8.2. E-Resident’s Digital ID

The e-residency program, established in 2014, involves issuing a **digital ID** (hereinafter e-resident’s digi-ID) to a trustworthy foreign citizen, which allows the person to access Estonian public and private sector e-services. The program aims to promote the development of Estonia’s economy, science, education, and culture. The validity period of the e-resident’s digi-ID is 5 years, after which a new digi-ID application must be submitted, a state fee paid, required documents provided, and a background check passed.

The e-resident’s digi-ID **is not** a travel document. It **does not grant** citizenship, tax residency, residence permit, or the right to enter Estonia or the European Union. It is **only usable in electronic environments**. The physical card of the e-resident’s digi-ID does not have a photo of the person and **cannot be used** for physical identification (see example). Also, being an e-resident **does not guarantee** obtaining a bank account in Estonia. To open a bank account, an application must be submitted to a credit institution, and the credit institution will conduct the required know-your-customer and anti-money laundering and counter-terrorism financing checks according to internal procedural rules. Most Estonian credit institutions (57%) do not distinguish e-residents from their regular clients, applying their usual due diligence measures to e-residents. However, 43% of credit institutions apply enhanced due diligence measures to e-residents.¹⁹⁷

¹⁹⁷ Survey conducted among representatives of credit institutions as part of the risk assessment preparation.

Figure 18. Sample of the e-resident's digital ID.

Source: PBGB

8.3. E-Residents and Entrepreneurship

A company can be registered in Estonia electronically through the e-Business Register portal or via a notary. The same options apply to both Estonian residents and e-residents. If an e-resident wishes to establish a legal entity that does not require a notary (e.g., a private limited company, non-profit association), the e-resident can establish the company using their digital identity in the e-Business Register portal, just like Estonian residents. If an e-resident wishes to establish a legal entity that can only be created through a notary (e.g., a public limited company, cooperative), the e-resident must also establish the legal entity through a notary.¹⁹⁸

Foreigners who are neither Estonian residents nor e-residents can create a company through an Estonian notary. Authorization is possible, meaning that a foreigner can authorize another individual or legal entity (e.g., a business service provider) with a notarized power of attorney to establish the company and does not need to come to the Estonian notary in person. Notarized powers of attorney certified abroad are also accepted. The notary uses a valid identification document to verify the identity of the founder or their representative and makes inquiries into national databases. During the notarial procedure, the same level of pre-checks (or post-checks) and background inquiries as in the e-resident's digital ID issuance process are not applied.

As of March 3, 2025, since the creation of the e-residency program, **122,000 e-resident digital IDs have been issued to foreigners**. Of these, **nearly 60,000 e-residents have a valid e-resident digital ID**. E-residents have been associated with a total of **43,000 Estonian legal entities**. As of March 3, 2025, **27,000 Estonian legal entities** are associated with individuals holding a valid e-resident digital ID, of which 21,000 are registered and 6,000 are deleted, bankrupt, or in liquidation. Of these 21,000 legal entities, approximately 54% are associated with EU citizens and 46% with third-country nationals.

When applying for an e-resident digital ID, applicants have predominantly indicated the creation of a company in Estonia as the main reason (73.1%). At the same time, 34% of valid e-residents have a business connection, and approximately 53% of companies established by e-residents were active. In 2024, the business register automatically deleted inactive companies. The main reason for this was the failure to submit annual reports. Of the companies associated with e-residents in the spring of 2023, 23% were deleted within a year and a half. Nearly a quarter, or 24%, of all companies historically associated with e-residents were deleted.¹⁹⁹

¹⁹⁸ Detailed instructions for establishing different types of legal entities can be found on the e-Business Register website. <https://ariregister.rik.ee/est/application/start>

¹⁹⁹ "Companies with Foreign Connections – One and a Half Years Later". FIU, September 2024. <https://fiu.ee/sites/default/files/documents/2024-10/V%C3%A4lismaalase%20seosega%20ettev%C3%B5tteid%20poolteist%20aastat%20hiljem.pdf>

Most e-residents are citizens of Spain, Ukraine, Germany, Turkey, and Finland. As a trend, it can be noted that e-residents from neighboring countries have established more companies than e-residents from countries geographically further away from Estonia, such as China or Japan. Since March 2022, initial e-residency digital IDs are no longer issued to citizens of Russia and Belarus. Therefore, Russian citizens are no longer among the top five countries of origin, and their number is decreasing over time²⁰⁰. Of the repeat applicants from Russia and Belarus, 70% receive a refusal decision, resulting in a linear decrease in their numbers over time.

8.4. E-Residency Risk Management

The risks of the e-residency program are managed regularly under the leadership of the EIS in the form of inter-agency coordination, involving all key stakeholders and supervisory authorities related to the program. To mitigate risks, pre-checks are applied to e-residency applicants and post-checks to e-residency holders. According to the law, the PBGB, ISS, TCB, and FIU²⁰¹ are competent to conduct state supervision over the use of the e-resident's digital ID.

Pre-Check

When submitting an application for an e-resident's digital ID, a foreigner must justify their application, complete a comprehensive application form, and undergo a background check. To receive the e-resident's digital ID, the applicant must appear in person at an Estonian foreign representation, where their identity is verified, and their fingerprints are taken. This means that biometric capture currently takes place when receiving the digital ID, not when submitting the application, but in the future, fingerprints will be taken already when submitting the document application. Biometrics and the data provided in the application are compared with data in national databases (e.g., the automatic biometric identification system and the identity documents database). Due to more effective pre-checks, the proportion of negative decisions increased **from 2% in 2018 to 10.9% in 2024**.

Until June 2023, it was possible to receive the e-resident's digital ID through an external service provider, as the network of Estonian foreign representations is limited. Through the external service provider (VTP), 1,365 e-resident digital IDs were issued. Upon discovering a breach of contract with the external service provider in May 2023, checks were initiated to determine whether the digital ID had ended up in the hands of the wrong persons due to the partner's actions. No cases were identified where the card had gone to the wrong person during the verification of all issued cards. All individuals who received the digital ID through the VTP are subject to regular post-check measures.

Post-Check

The PBGB has developed various capabilities to monitor and analyze the behavior of e-residents and their use of the e-resident's digital ID. If undesirable activity is detected, the e-resident's digital ID is invalidated. Since June 2022, the PBGB has been using an automated post-check solution that allows for regular and automatic checks of risk information related to e-residents from both national and European Union databases. While 29 e-resident digital IDs were invalidated as a result of post-checks in 2020, this number was 227 in 2024.

²⁰⁰ As of April 14, 2025, there are 2,060 Russian citizens and 504 Belarusian citizens with a valid e-residency digital ID among e-residents. In total, there are 60,310 valid e-residency digital IDs. Russian and Belarusian citizens make up 4.3% of valid e-residents. For comparison, in March 2022, when the acceptance of new e-residency applications from Russian and Belarusian citizens was suspended, their share was 9%.

²⁰¹ The Act amending the Identity Documents Act and related laws was adopted by the Parliament (Riigikogu) in June 2025.

8.5. Companies with E-Residents in ML Statistics

8.5.1. E-residents in FIU Statistics

From 2020 to 2024, **5.4%** of the reports submitted to the FIU involved an e-resident or a company associated with them as the party to the suspicious transactions. Of all e-residents²⁰², **1.5%** and **5.8%** of the Estonian companies associated with them appeared in FIU reports at least once. Reports concerning e-residents and their established companies were used in information forwarded to other authorities in **11.7%** of cases, which is a somewhat higher forwarding rate than for other FIU reports. This indicates that reports concerning e-residents and their companies contain slightly stronger indications of suspicious activity than average.

On average, **53%** of all reports concerning an e-resident or a company associated with an e-resident came from foreign countries. During the same period, **23.4%** of all substantive money laundering suspicion reports from foreign authorities involved either an e-resident or a legal entity established or associated with them. These two facts suggest that **e-residents and their companies have primarily been involved in money laundering suspicion activities abroad.**

Since 2022, the proportion of information from other countries in reports concerning e-residents has started to decline (falling to 45% in 2024), while **the proportion of reports made by Estonian credit institutions (and to a lesser extent financial institutions) has significantly increased. The main reasons for these reports point to suspicious transactions or assets of unclear origin.**

At the same time, since 2022, the number of money laundering suspicion reports submitted by Estonian credit institutions has generally increased (not only in connection with e-residents). This indicates that Estonian credit institutions have generally started to apply stronger due diligence measures, and during the application of these measures, more e-residents and their associated legal entities have been flagged.

The **main keywords in all reports concerning e-residents** and their established or associated companies are possible fraud, tax violations, and assets of unclear origin.

Based on the data from the 2023 study on foreigners²⁰³ conducted by the FIU, the following groups of legal entities were compared (based on the data from the Business Register as of April 30, 2023):

1. Legal entities associated with individuals holding a valid e-resident digital ID as of April 30, 2023;
2. Legal entities associated with other non-residents;
3. Legal entities associated only with Estonian residents.

From 2020 to 2024, these groups of legal entities appeared in FIU statistics as follows:

- On average, 1.4% of all Estonian legal entities (hereinafter “companies”) appeared in FIU reports.
- Estonian companies associated with foreign individuals appeared in FIU reports more frequently than Estonian companies associated only with Estonian individuals (2.8% vs. 1.0%).
- Of the companies associated with individuals holding a valid e-resident digital ID, 2.3% appeared in FIU reports, which is a smaller proportion than the appearance rate of all Estonian companies associated with non-residents in FIU reports (2.8%).
- The highest money laundering risk comes from Estonian companies with a foreign beneficial owner (3.2% of the companies in this group registered in the Business Register appeared in FIU reports), followed by the group of Estonian legal entities associated with other non-residents (3.1% of this group appeared in reports).

²⁰² Here, all individuals who have held e-residency during the period 2014–2025 are meant.

²⁰³ FIU’s study on foreigners, January 2024: <https://fiu.ee/valismaalased-est-ettevotetes>

8.5.2. E-residents in TCB statistics

The TCB annually assesses the risks of approximately 26,000 legal entities associated with e-residents using an automatic risk model and checks around 370 legal entities associated with e-residents. As a result, a proposal is made to either refuse or revoke approximately 170 e-resident digital IDs.

The main violation leading to the proposal is the misuse of the VAT registration number. **In terms of money laundering, this is one typology associated with e-residents, where tax fraud is a predicate offense for money laundering** (see cases 1 and 2), where Estonian legal entities were used as intermediaries in a cross-border tax fraud scheme, and the prerequisite was the existence of a valid VAT registration number.

The TCB does not base its risk models on the connection of the legal entity, i.e., it does not matter whether the legal entity is associated with an e-resident, another non-resident, or an Estonian person. Legal entities are dealt with based on their risk level, and high-risk individuals are directed to control.

In the 2023 study on foreigners by the FIU, the following groups of legal entities were distinguished and appeared in TCB statistics from 2020 to 2024:

- The most legal entities that needed to be checked were those associated with non-residents (who are not e-residents). On average, 2% of all legal entities associated with non-residents (who are not e-residents) needed to be checked annually. This was followed by legal entities associated with Estonian persons (1.5% of the group) and legal entities associated with e-residents (1.4% of the group).
- The situations where the control ended with an increase in the tax amount were most common for legal entities associated with Estonian persons (on average 63% of all controls carried out on legal entities associated with Estonian persons). This was followed by legal entities associated with non-residents (who are not e-residents) (45% of the controls carried out on them) and legal entities associated with e-residents (25% of the controls carried out on them).
- The proportion of violations in controls related to the VAT registration number was highest for legal entities associated with e-residents (on average 49% annually of all legal entities associated with e-residents that committed violations). This was followed by legal entities associated with non-residents (who are not e-residents) (31%) and legal entities associated with Estonian persons (24%).

CASE 1:

According to the investigation, the suspects established companies in 15 EU member states that operated as legitimate suppliers of electronic goods. Through online stores, electronic devices worth over 1.48 billion euros were sold to customers within the EU. Although end consumers paid VAT on their purchases, the companies selling the goods did not fulfill their tax obligations. By abandoning the companies, the transfer of unpaid tax amounts to various national tax authorities was avoided. Other links in the fraud chain then claimed VAT refunds from national tax authorities, causing an estimated **VAT loss of 297 million euros**. The proceeds from the criminal activity were moved to offshore accounts. Among other things, **11 Estonian private limited companies (OÜs) with no real economic activity were used to move the funds, involving 13 e-residents**.

CASE 2:

Since 2017, a brokerage company in one EU country has been running various VAT fraud schemes related to the sale of electronic goods. In 2020, the same VAT fraud scheme organizers entered the protective mask market. The supply chain, led by the criminal organization, used shell companies, straw men, and fictitious identities in various countries, including Hong Kong and the relevant EU country. According to the investigation, neither the company at the beginning of the supply chain nor the company in Hong Kong paid VAT on the amounts they received from selling face masks to the ministry of the EU country. **Currently, it is known** that two Estonian private limited companies (OÜs) were involved in the scheme, one of which had a foreign e-resident as a board member. The Estonian OÜ had no real activity. The scheme is estimated to have defrauded up to **195 million euros**. The pre-trial investigation is still ongoing.

8.5.3. E-residents in PBGB statistics

According to the PBGB statistics, from 2020 to 2024, there have been a **total of 78** e-resident digital IDs revoked due to possible money laundering or suspicion of money laundering. The increase in the number of cases has been largely aided by the automated control introduced in 2022. In the money laundering-tagged foreign inquiries received by the PBGB from 2021 to 2024, 113 companies²⁰⁴ were involved, **31%** of which were associated with e-residents. Additionally, inquiries were made about nine e-residents.

The companies mentioned in the foreign inquiries sent to Estonia are characterized by the fact that, in many cases, a single company is associated with various types of individuals, including Estonian citizens, e-residents, and other non-residents. Generally, it can be said that half of the inquiries were made about companies associated with Estonian citizens, and the remaining half was divided between 30% associated with other non-residents and 20% associated with e-residents.

8.5.4. ML suspicion inquiries involving companies with e-residents

In 2024, 88 foreign inquiries related to e-residents were entered into the PBGB information system, of which 50 were about e-residents and 38 about companies associated with e-residents. The countries of origin of the e-residents were 21, with most inquiries concerning e-residents from Ukraine, Germany, and Russia. The main cases involved fraud or money laundering incidents related to the e-resident or their company, where funds had moved through or to Estonia.

²⁰⁴ This is partial data, as the personal or registration code of the party was indicated in only 44% of the queries.

In 2024, the TCB identified violations of export restrictions against Russia in 14 cases. The violations were mostly associated with Estonian e-residents or their companies with Russian, Belarusian, and Israeli citizenship. These violations indicate that enhanced background checks for Estonian e-residents with backgrounds from these countries are necessary and justified to prevent potential money laundering and predicate offenses using e-residency²⁰⁵.

Table 78. Foreign inquiries received by the PBGB regarding e-residents from 2020 to 2024

Year	Number of inquiries for natural persons	Number of inquiries for legal persons	Total inquiries
2020	68	63	131
2021	51	82	133
2022	67	92	159
2023	51	68	119
2024	50	38	88

Source: PBGB

According to the PBGB, the number of foreign inquiries decreased by 25% in 2023 compared to 2022, which may be due to the fact that since June 16, 2023, queries can also be entered into the information system retrospectively. From 2020 to 2024, foreign inquiries were received regarding both natural and legal persons, mainly concerning fraud, money laundering, and criminal proceeds. Most inquiries were related to the use of an e-resident's company for illegal activities, such as using the company's bank account for money laundering. In 2023, most foreign inquiries were received concerning e-residents with Russian, Ukrainian, Polish, and Latvian citizenship. Compared to 2022, the number of inquiries concerning Latvians decreased threefold, while the number of inquiries concerning Russians increased by 20%.

8.5.5. E-residents in criminal proceedings and court cases

From 2020 to 2024, the PBGB handled 66 criminal cases where at least one criminal episode was marked as money laundering. Of the 66 criminal cases, five involved an e-resident or a legal entity associated with an e-resident. Of the five proceedings, one was terminated, and one was reclassified as a crime related to the handling of strategic goods. The remaining three were related to money laundering of funds obtained from tax crimes committed in Estonia, international investment fraud, and cybercrime.

Table 79. Court Cases on ML and Criminal Proceedings Involving Companies with E-Residents from 2020 to 2024

	Number of Companies with E-residents
Court Cases	1
Criminal Proceedings	5

Source: PBGB

²⁰⁵ E-residency situation overview 2024.

In Estonia, the principle of double jeopardy (*ne bis in idem*) applies. This does not preclude conducting an investigation in Estonia, but generally, the initiation of criminal proceedings and preliminary investigation falls under the jurisdiction of the country where the crime was committed or where the perpetrator resides. **Most often, the e-resident suspected of crimes abroad does not physically operate in Estonia, and their companies lack local (economic) activity and bank accounts, meaning the suspicious activity is not carried out in Estonia.**

The status of an e-resident or the registration of a company in the Republic of Estonia does not necessarily provide grounds for initiating proceedings. According to § 6 of the Penal Code, the Estonian Penal Code applies to acts committed on Estonian territory. An exception is made by § 7 of the Penal Code, which allows for the initiation of criminal proceedings for crimes committed abroad if the victim or suspect is an Estonian citizen or a legal entity registered in Estonia. However, this provision is used only if initiating criminal proceedings for such crimes is justified, meaning the criminal proceedings would be faster and more effective in Estonia. In the situations described above involving legal entities associated with e-residents, the proceedings require the collection of evidence mainly in other countries. **Therefore, it is not possible to quickly and effectively handle the described crimes in Estonia, and they are generally not initiated.** In the case of a crime committed outside the territory of the Republic of Estonia, the decision to initiate or review the justification of the decision is made only by the Prosecutor General's Office (§ 435 (3) of the Code of Criminal Procedure).

In summary, the very small number of criminal cases related to money laundering in Estonia reflects the main *modus operandi* associated with companies of e-residents. This is also confirmed by the assessment of the Prosecutor General's Office, according to which inquiries about e-residents and their companies are one of the main legal assistance requests received by the Estonian Prosecutor General's Office from other countries. **Most foreign inquiries about e-residents' companies are related to fraud committed abroad.**

The small number of criminal proceedings is also reflected in court decisions. From 2020 to 2024, a total of 31 court decisions were finalized in Estonia, where at least one charge was money laundering (§ 394 of the Penal Code). In 29 of these cases, the perpetrator or channel for money laundering was an Estonian legal entity. Of these, only one proceeding was related to a company associated with an e-resident, where the layering of funds obtained through business fraud²⁰⁶ occurred in Estonia. In this case, the e-resident lived in Estonia.

8.6. Trends and Summary

E-residency allows foreigners to register a company in Estonia and perform other official actions, which means there is a risk that the use of such a service may lead to abuses. E-residency itself does not create new money laundering and terrorist financing risks from the perspective of **non-residents**, but it can make committing offenses easier and cheaper – thus more attractive. E-residency, in conjunction with the ease and speed of establishing a company in Estonia, the business-friendly tax environment, and the extensive network of business service providers, can be an additional risk for the misuse of legal entities for money laundering purposes, primarily outside Estonia. This is illustrated by the information from the FIU, the PBGB, and the Prosecutor General's Office, where a significant proportion of inquiries or reports from foreign authorities are related to e-residents or their associated companies. **This means that the risks associated with e-residency in terms of money laundering are mainly related to the misuse of companies established in Estonia in other countries.** There are very few cases where an e-resident or their company becomes a party to criminal proceedings in Estonia. Consequently, the number of court decisions involving e-residents and money laundering in Estonia is essentially non-existent.

²⁰⁶ BEC – business e-mail compromise.

Based on the statistics from the FIU, it can be said that 98.5% of all e-residents and 94.2% of all e-resident companies **have not been involved** in activities that increase the risk of money laundering. However, the described cases show that even with the involvement of just one or two e-residents, it is possible to create international criminal schemes that can cause significant damage (mostly in other countries). Even if the economic damage caused by these schemes does not occur in Estonia and other foreigners are involved in the scheme alongside e-residents, such cases can cause considerable reputational damage to Estonia. For example, in the described cases, Estonian companies were used, which had no real economic activity in Estonia, meaning that the supervision of companies without signs of activity is important.

A persistent issue is the ability to conduct background checks on applicants from third countries. Since Estonia often lacks any judicial, security, or law enforcement cooperation with these countries, it is not possible to fully ensure that there are no circumstances that would preclude the issuance of e-residency. This risk is mitigated by the direction taken in the e-residency continuation strategy (2022–2025), which generally does not offer e-residency to citizens of countries that pose a significant security or e-resident digital ID misuse risk. Additionally, since March 2022, new e-resident cards are no longer issued to citizens of Russia and Belarus.

As an additional risk, supervisory authorities see the trend where e-residents use the authentication capabilities created with the digital ID even after the expiration of the e-resident digital ID. This risk is being mitigated through the harmonization of validity periods.

Several steps were taken from 2020 to 2024 to reduce the money laundering and terrorist financing risks associated with e-residency:

- As a significant preventive measure, the e-residency continuation strategy (2022–2025) focused on target countries with which there is professional cooperation.
- The pre-check of e-residency applicants has improved, resulting in the proportion of negative decisions rising from 2% to 10.9% over the past six years.
- In 2021, the PBGB introduced a new e-resident digital ID e-application environment, which allows for more information about the applicant's background and intentions.
- Since 2022, an automated post-check solution has been applied, resulting in an increase in the number of invalidated e-residency digital IDs from 29 in 2020 to 227 in 2024. Additionally, the PBGB's information exchange with cooperation partners has improved, resulting in an increase in the number of e-residencies invalidated due to money laundering suspicion.
- In 2023, the issuance of e-resident digital IDs through an external service provider was discontinued.
- In 2023, the PBGB introduced a risk profile solution that enhances background checks. The data exchange between the PBGB and the TCB was also improved.
- The post-check of e-residents' business activity is conducted more frequently compared to 2020. This is supported by the more extensive deletion of legal entities that failed to submit annual reports from the business register, which began in 2024.
- The risk level associated with VASPs created by e-residents, which was high in 2020, has now significantly decreased. This was aided by the strong regulation of the VASP market in Estonia.

4. ANNEXES

Annex 1. List of Predicate Offenses for ML

1. § 209. Fraud
2. § 213. Computer Fraud
3. § 184. Illegal Handling of Narcotic and Psychotropic Substances in Large Quantities
4. § 3891. Concealment of Tax Liability and Unjustified Increase of Refund Claim
5. § 211. Investment Fraud
6. § 217². Abuse of Trust
7. § 384. Causing Insolvency
8. § 298. Giving Bribes
9. § 214. Extortion
10. § 296. Mediation of Bribes
11. § 391. Smuggling
12. § 372. Unauthorized and Prohibited Economic Activity
13. § 931. Violation of International Sanctions and Government of the Republic Sanctions
14. § 294. Accepting Bribes
15. § 201. Embezzlement
16. § 376. Violation of the Rules for Handling Tobacco Products
17. § 210. Subsidy Fraud
18. § 188. Illegal Cultivation of Poppy, Cannabis, and Coca Bush
19. § 418. Illegal Handling of Firearms, Their Essential Parts, and Ammunition
20. § 202. Acquisition, Possession, and Marketing of Property Obtained Through an Offense
21. § 418¹. Illegal Handling of Firearms, Their Essential Parts, and Ammunition Prohibited in Civil Circulation

22. § 255. Criminal Organization
23. § 256. Organization of a Criminal Organization
24. § 212. Insurance Fraud
25. § 199. Theft
26. § 300¹. Violation of Operational Restrictions
27. § 217. Illegal Access to a Computer System
28. § 361. Damage to Natural Fauna
29. § 2342. Espionage and Support of Espionage Against the Republic of Estonia
30. § 200. Robbery
31. § 206. Interference with Computer Data
32. § 232. Treason
33. § 133. Human Trafficking
34. § 233. Non-Violent Activities Against the Republic of Estonia by a Foreigner
35. § 235¹. Relationship Against the Republic of Estonia
36. § 237. Terrorist Offense
37. § 237¹. Terrorist Organization
38. § 237². Preparation and Incitement of a Terrorist Offense
39. § 237³. Financing and Supporting Terrorist Offenses and Activities Aimed at Committing Them
40. § 368¹. Violation of Requirements for Transboundary Waste Shipment
41. § 393. Illegal Operations with Duty-Free and Excise Goods
42. § 402³. Accepting Bribes in the Private Sector
43. § 402⁴. Giving Bribes in the Private Sector
44. § 415. Illegal Handling of Explosive Devices and Their Essential Parts
45. § 421¹. Illegal Transport of Strategic Goods and Illegal Provision of Services Related to Strategic Goods
46. § 421². Transport of Prohibited Strategic Goods and Provision of Services Related to Prohibited Strategic Goods
47. § 421³. Illegal Handling of Demilitarized Military Goods



REPUBLIC OF ESTONIA
MINISTRY OF FINANCE