Republic of Estonia
Financial Intelligence Unit

2025 YEARBOOK



Estonian Financial Intelligence Unit Yearbook 2025
Translation: Välek OÜ
Designed by: Age Reklaam OÜ
Cover photo: Kaupo Kalda
Illustrations: Age Reklaam OÜ & Shutterstock

The Financial Intelligence Unit
Pronksi 12, 10117 Tallinn

ISSN 2806-3104 (in print)
ISSN 2806-1934 (electronic edition)

CONTENTS

Foreword 4
2025 timeline 8
Prevention of money laundering 10
- Money laundering risk profile 10
- Reporting 17
- Co-operation in the prevention of money laundering 22
- Disposal restrictions and administrative confiscation 28
- Money laundering convictions 33

Countering terrorist financing 36
- Risk profile 36
- Terrorist financing reports 38
- Best report of the year 41

International financial sanctions 44
- Risk profile 45
- Reporting 46
- New restrictions and regulations 48
- Implementation of financial sanctions and ensuring their lawful application 50
- Proliferation financing 54

Authorisations and supervision 57
- Authorisations 57
- Supervision 60
  - Financial institutions 62
  - Providers of company services 66
  - Gambling operators 69
  - Virtual currency service providers 71

About the Financial Intelligence Unit 75
- Role 75
- Organisational development and implementation of strategy 79

5 years in numbers 84
References and further reading 86



Photo: Vahur Lõhmus

DEAR READER!

I AM PLEASED TO INTRODUCE THE 2025 YEAR-BOOK.

About a month ago, the Estonian Government appointed me to a second term. This is a great honour and a significant responsibility. I would like to thank you for the trust placed in me.

The process for selecting the head of the Financial Intelligence Unit (FIU) ensures the autonomy and independence of the authority. The appointment of a suitable candidate is first decided by an independent Committee for Selection of Top Managers, then by the minister in charge of the policy sector and finally by the Estonian Government.

Autonomy and independence are the most important safeguards for financial intelligence units. In 2025, the global umbrella organisation of financial intelligence units, the Egmont Group, updated its requirements on autonomy and independence and set out 18 criteria as a core part of the co-operation framework defining when a financial intelligence unit can be considered autonomous and independent. According to these criteria, autonomy and independence are not merely nominal, but must be underpinned by genuine safeguards. This also

entails the responsibility to organise internal operations independently and autonomously to prevent political influence, arbitrary decision-making by officials and the carrying out of inquiries or analyses without a legal basis, among other things. Autonomy and independence are a prerequisite for our participation in the Egmont Group network and for exchanging information with international partners. Without these, we would be unable to navigate the international anti-money laundering system. This is particularly important given that international money laundering poses the greatest risk to our economic and financial systems.

Financial intelligence units must be autonomous and independent worldwide.

The Financial Intelligence Unit has had a busy year, as never before have we been so prominently in the public spotlight. Naturally, this has required a great deal of explanation and effort from the entire team, but we see this as an opportunity. The Financial Intelligence Unit has become more prominent in public awareness as an authority, which enables us to explain our role in society. Our primary function is not to prevent money laundering through supervision, because when supervisory mechanisms are in place, we do not expect market participants to be our greatest money laundering risk. We must therefore keep our main focus on detecting and preventing criminal offences. Money laundering, like the criminal activity that precedes it, is often covert in nature. It is a hidden form of crime in which there is no victim or in which the victim does not report the offence. This is precisely what financial intelligence units must uncover outside of criminal proceedings.

I have explained the issues surrounding the request for bank account statements and the necessity of such data in several opinion pieces, articles and radio and television appearances, so I will not repeat those arguments here. We understand public concern regarding the potential misuse of the system and the processing of information relating to persons who have not made transfers or transactions indicative of criminal activity. We also recognise that, to provide reassurance, the system must have effective controls in place. To this end, the legislator has already established both internal and external security measures, and joint proposals from the Ministry of Finance and the Financial Intelligence Unit are expected to further strengthen these controls. However, this is contingent upon the Parliament of Estonia (Riigikogu) approving these proposals. We also hope that the Riigikogu will renew our mandate in full to avoid similar doubts in the future.

At the same time, we have accomplished a great deal at the Financial Intelligence Unit and we are pleased to present this in the Yearbook. In addition to 2025, we are also providing a summary of the past five years, which marked our first strategic period. We have established data processing rules and set up an internal control and quality assurance system that meets modern requirements. Notably, we have published dozens of risk analyses, provided guidance to market participants and trained thousands of people. We have adopted an open approach towards the market, hold annual co-operation meetings with major market participants and provide advance notice of inspections several months beforehand.

In five years, supervision has shifted from a one-way approach to a dialogue with market participants.

Alongside this, many market participants have made significant progress over the past five years. The private sector increasingly understands its role in the anti-money laundering system and the types of potential misuse it must guard against. Market participants submit reports with references to money laundering typologies that they have read about in our advisories or heard about during training sessions. A good example is a market participant that was initially resistant at the start of the supervisory dialogue, but upon realising that the Financial Intelligence Unit actually wanted to help, improved its processes. We gained confidence in the commitment of the market participant and the participant, in turn, was able to improve its systems. Only by working together can we prevent money laundering and ensure security.

We are regarded as a respected partner in Europe and globally, and it has been said that co-operation with us is better than ever before. We have reached a point where our staff are progressing not only within the financial sector, but also internationally. We are pleased, but also sorrowful, that one of the most experienced staff members of the FIU, Deputy Head Markko Kard, is moving to the EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). He will have the opportunity to shape a substantial body of regulations – nearly 40 Level 2 and Level 3 measures – which AMLA will make mandatory for both the private and public sectors in the coming years.

Five years ago, when I was appointed Head of the Financial Intelligence Unit, the FIU had just been established as an authority separate from the Police and Border Guard Board. A similar trend can also be seen in Europe where systems have been rapidly reformed in response to anti-money laundering incidents or major issues, with the move towards standalone financial intelligence units forming one of the cornerstones of this approach.

For example, Latvia was still in a state of full crisis in 2018 when it was at risk of being placed on the FATF grey list. The entire country rallied behind its Financial Intelligence Unit, which reported directly to the Prime Minister. The FIU was made a standalone authority and provided with the necessary tools and resources. All competent authorities made efforts to understand the content of the standards and best practices, and did their utmost to ensure that the country would be effective in the next assessment or, why not, even become the most effective anti-money laundering country in the world. Seven years later, a new report on Latvia was published, positioning it as the leading country globally in the fight against money laundering, characterised by a very good understanding of risk, a strong financial intelligence unit, a high number of risk-based money laundering criminal proceedings and approximately 320 million euros confiscated over five years.

Although the evaluation of Estonia will likely not take place until 2030 or 2031, the evaluation process is already underway, as today's actions are taken into account in the evaluation results. In the previous round, we passed the evaluation by a narrow margin and did not end up on the so-called grey



list. The MONEYVAL evaluation provided us with a clear roadmap; however, we must acknowledge that post-evaluation progress requires renewed momentum. A simple example is confiscation: in recent years, this figure has remained between 4 and 6 million euros annually, which is far below the five-year total of Latvia of 320 million euros.

Among European countries, Serbia, Malta, Bulgaria, Croatia and others have been on the grey list. In 2021, the International Monetary Fund (IMF) explained that inclusion on the grey list means a decline in a country's gross domestic product (GDP) ranging from 4.6% to 10.6%. In addition to the decline in GDP, the cost of money on capital markets would increase, meaning that the money we would need to borrow to finance a 4.5% budget deficit would carry significantly higher interest rates. Banks may lose correspondent relationships, which would make settlement in certain currencies impossible. Estonian people would not be able to open accounts with financial institutions in other countries or it would take weeks or months to do so. Foreign investment would also decline. Malta is no longer on the grey list as of 2022 but the country is still feeling the economic impacts.

Time is of the essence, and national capacity depends on implementing the necessary changes without delay and in full.

Therefore, as a country, we must quickly decide on our future path, as we can no longer afford to lose time. These are shared roadmaps, narratives and ideas for how to make the state more efficient. In geopolitically uncertain times, political understanding of the importance of this issue and support for it are more crucial than ever. I would not want us to be looking for scapegoats again during the next MONEYVAL evaluation, as happened in the wake of the Danske Bank scandal.

The Financial Intelligence Unit has become a centre of excellence and a leader in its field, and we are ready to move our country forward, but to do so, we must have the necessary rights and competencies. As a country, we must be aligned.

I hope you find this Yearbook interesting.

Watch the presentation of the Head of the Financial Intelligence Unit at the EFIUC 2025 conference (in Estonian)



Matis Mäeker
Head of the Estonian Financial Intelligence Unit

2025 TIMELINE

JANUARY

- On 1 January, the International Sanctions Act entered into force, imposing a reporting **obligation on persons with special obligations** for the submission of data which is necessary for the implementation and application of the financial sanction.
- On 13–14 January, a meeting of the Financial Action Task Force (**FATF**) Eurasia, Middle East and North Africa (EMENA) working group was held in Tallinn, where progress by Bulgaria and Croatia, both of which are on the grey list, was discussed.
- From 29 January to 2 February, meetings of the **Egmont Group**'s European regional working groups and regional groups were held in Malta where, among other things, the importance of strategic analysis was emphasised. The financial intelligence units of Estonia and Japan concluded a long-prepared co-operation agreement.
- From 27 January to 7 February, the interim meeting of the **Egmont Group** was held virtually. Prior to this, infringement proceedings had been initiated against Colombia in relation to the unauthorised transmission and disclosure of information received from a foreign country.

FEBRUARY

- On 24 February, the European Union (EU) adopted its **16th package of sanctions**, adding a Russian virtual asset service provider Garantex to the list. Its subsidiary, Garantex Europe OÜ, held an Estonian virtual asset service provider's authorisation until 24 February 2022. In addition, a further 13 Russian banks were removed from the SWIFT system, which facilitates international payments.

MARCH

- On 7 March, the Financial Intelligence Unit issued guidelines on the obligations of **virtual currency service providers** and the application of due diligence measures in correspondent relationships with financial institutions.
- On 11 March, the Head of the FIU participated in the first meeting of the General Board of the EU Authority for **Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)** in Frankfurt where the members of the AMLA Executive Board were appointed and the rules of procedure adopted.
- On 31 March, the Supreme Court of Estonia rendered a judgment refusing to grant permission for the **transfer of property suspected of money laundering to state ownership** and clarified the conditions under which property suspected of money laundering may be transferred to state ownership during administrative proceedings without anyone having been convicted of money laundering in criminal proceedings.

MAY

- On 13–14 May, a meeting of the **AMLA** General Board was held where preparatory work related to the secondment of delegates from financial intelligence units to AMLA was discussed.
- On 14 May, the EU adopted its **17th package of sanctions**, which expanded the list of companies subject to export restrictions and the list of vessels subject to service restrictions.
- From 27 to 30 May, the **OECD Working Group on Bribery** visited Estonia to assess the country's capacity to prevent and prosecute bribery offences in international commercial transactions.
- The Financial Intelligence Unit published an updated **financial sanctions guideline** for persons with special obligations, providing an overview of financial sanctions and examples of ways in which they can be violated, and introduced a new recommended form for derogation authorisation applications. The second guideline is intended for persons subject to the supervision of the FIU and sets out how to mitigate risks related to the violation or circumvention of a financial sanction, both through the establishment of appropriate organisational structures and the application of due diligence measures.

JUNE

- On 10–14 June, the **MONEYVAL** Plenary was held where the evaluation report on Latvia was approved, along with amendments to FATF standards and procedures. Decisions were also adopted regarding mutual evaluations, supervisory proceedings and lists of countries under enhanced monitoring.
- On 12 June, the Supreme Court of Estonia rendered a judgment **allowing property suspected of money laundering to be transferred to state revenue**.
- On 18 June, a meeting of the **AMLA** General Board was held online where the primary rules of procedure of the authority were discussed.

JULY

- On 18 July, the EU adopted its **18th package of sanctions**. In the financial sector, a full ban on transactions was introduced for Russian and Belarusian banks, and 22 Russian banks, along with two Chinese banks, were added to the sanctions list.
- From 6 to 11 July, the **Egmont Group** Plenary was held in Luxembourg, with the main focus on succession and sustainability within financial intelligence units.

AUGUST

- On 28 August, **AMLA** Chair Bruna Szego visited Estonia together with Janneke de Smet-Dierckx, Lead of the Financial Intelligence Units pillar. Representatives of the Financial Intelligence Unit, the Financial Supervision Authority, the Ministry of Justice and Digital Affairs, and the Estonian Bar Association participated in the meetings. Discussions focused on the main risks of money laundering and terrorist financing, national challenges in transposing the EU Anti-Money Laundering Directive, EU-wide supervisory convergence and the specific features of non-financial sector supervision.

SEPTEMBER

- On 15–16 September, the Financial Intelligence Unit organised a **training session of FATF standards** for public sector partner institutions, delivered by internationally recognised consultants.
- As of 30 September, **EU restrictive measures** against Iran were reinstated, following Iran's non-compliance with the terms of the nuclear agreement.

OCTOBER

- On 6 October, the Ministry of Finance published the **national money laundering and terrorist financing risk assessment**, which indicates a medium level of risk for both money laundering and terrorist financing in Estonia. More than ten employees of the Financial Intelligence Unit and many representatives from other agencies contributed to the risk assessment.
- For the second consecutive year, the **Estonian Academy of Security Sciences** has been offering the elective course 'Money Laundering and its Prevention Measures', which is co-ordinated and largely delivered by the Financial Intelligence Unit.
- On 14 October, an **AMLA** meeting was held where issues related to the information system, evaluations and mutual assistance were discussed.
- On 23 October, the European Union adopted its **19th package of sanctions**, which, among other things, banned transactions involving certain crypto-assets in the virtual currency sector and prohibited the provision of crypto-asset services to Belarusian persons and companies.
- Peaasi once again recognised the Financial Intelligence Unit as an **organisation that values mental health**, this time with the 'Blooming' label.

NOVEMBER

- On 3–5 November, the **Financial Intelligence Unit Conference** 2025 was held, featuring 22 experts from Estonia and abroad. In a parallel training session, representatives of the private and public sectors addressed a sample case study on anti-money laundering.

DECEMBER

- On 4 December, the Financial Intelligence Unit published an analysis identifying a systemic risk among **virtual currency service providers** related to the identification of correspondent relationships and the application of due diligence measures. The analysis included contributions from the US Financial Crimes Enforcement Network (FinCEN) and garnered international attention.
- On 9 December, an analysis by the Financial Intelligence Unit drew attention to potential vulnerabilities among **non-governmental organisations** in relation to terrorist financing.
- On 9 December, a meeting of the **AMLA** General Board took place where a proposal for the appointment of the Executive Board member of the Authority to the European Parliament was adopted.
- On 15–19 December, the MONEYVAL Plenary was held, during which the Deputy Head of the Financial Intelligence Unit Laura Aus was elected as a MONEYVAL Bureau member. The two-year term of the Head of the FIU Matis Mäeker as Vice-Chair of MONEYVAL came to an end.

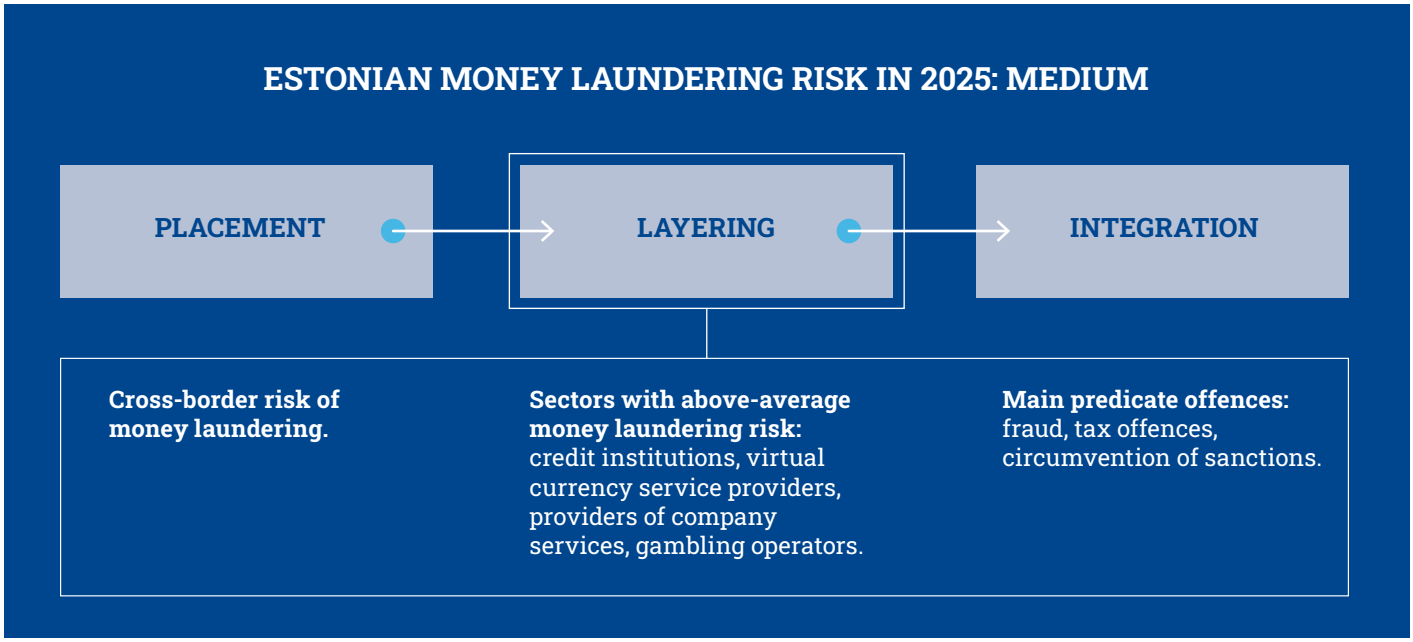


PREVENTION OF MONEY LAUNDERING

MONEY LAUNDERING RISK PROFILE

There have been no fundamental changes in the money laundering risk profile of Estonia over the past five years. The main threat is the layering of proceeds originating from predicate offences committed abroad, ie their laundering through Estonia. This involves Estonian persons who allow their company or personal bank accounts to be used to move illicit proceeds through Estonia, including into crypto-assets, or to withdraw them in cash. We can see that the criminals benefitting from these activities include persons from both abroad and Estonia. Proceeds from crime continue to be integrated, to some extent, into real estate in Estonia and abroad.

Money laundering methods are constantly evolving.



Over the past five years, money laundering methods have evolved significantly. Money laundering is often carried out across multiple banks, with, for example, up to ten bank accounts in Estonia and abroad being used. In addition, laundering is carried out by professionals and by seemingly unrelated persons who have opened accounts with credit institutions and virtual currency service providers to cover their tracks. Structuring is also used, whereby a large transaction amount (which would attract attention during an audit) is divided into several smaller, interconnected amounts.

ESTONIAN NATIONAL RISK ASSESSMENT

On 30 September 2025, the AML/CFT Governmental Committee approved a three-part national risk assessment report identifying the threats and vulnerabilities related to money laundering, terrorist financing and proliferation financing in Estonia.

The money laundering risk assessment also found, among other things, that, at the sectoral level, threats and vulnerabilities have increased among providers of company services and gambling operators.[1]

A threat is an event, activity or pattern of behaviour indicating a possibility that financial criminals are using the economic space and financial system of Estonia to launder their proceeds. Vulnerability assesses the effectiveness of measures of the anti-money laundering system as a whole.

Sector	Money laundering threat level	Vulnerability level	Residual risk level
Credit institutions	medium-high	medium	medium
Creditors and credit intermediaries	medium	medium	medium
Investment firms	medium	medium	medium
Payment institutions and e-money institutions	medium-high	medium	medium
Management companies	medium	medium-high	medium-high
Assurance undertakings	low	low	low
Savings and loan associations	medium	medium	medium
Currency exchange providers	medium	medium-low	medium
Virtual currency service providers	medium-high	medium-high	medium
Gambling operators	medium-high	medium-high	high
Attorneys	medium	medium	medium
Notaries	medium	medium	medium
Providers of accounting or tax advice services	medium	medium	medium
Legal service providers	medium	medium	medium
Traders	medium-low	high	medium
Precious metal dealers	medium-low	medium	medium
Estate agents	medium	medium-high	medium
Audit firms	low	medium-low	low
Company service providers	medium-high	medium-high	medium
Enforcement agents and bankruptcy trustees	low	medium-low	low
Pawnbrokers	low	medium	low

Source: Estonian Ministry of Finance[1]

The Ministry of Finance co-ordinated the preparation of the risk assessment, which involved nearly 120 experts from the public and private sectors. The Financial Intelligence Unit was responsible for leading three working groups, with nearly twenty members of staff participating in the process.

Following the risk assessment, the relevant authorities prepared an action plan, which, like the risk assessment, was approved by the AML/CFT Committee.

KEY PREDICATE OFFENCES TO MONEY LAUNDERING

As in 2020, we were faced with a pandemic in 2025. While COVID-19 disrupted society five years ago, in 2025 the term 'epidemic' was sometimes used in the media and in meetings between institutional representatives when referring to **fraud**.

In the 2024 yearbook, we warned that fraud schemes are becoming increasingly complex, more widespread than organised crime and that the associated losses can amount to tens of millions of euros annually. Therefore, a more comprehensive approach is needed, rather than addressing individual cases in isolation. In 2025, the total losses from fraud doubled compared to 2024, reaching 29 million euros. This includes only cases known to the police, although the actual situation is significantly more serious.

In the cases analysed, the Financial Intelligence Unit observed that Estonian persons are used to launder proceeds from fraud committed abroad – this serves as an intermediary stage, as criminal proceeds and other leads are quickly moved abroad. Both call centres and the organisers of criminal schemes are located there. The range of countries where predicate offences are committed is wide. As with fraud, the subsequent money laundering chain is international and organised, involving persons and accounts in multiple countries. With fast payment methods, money can quite literally, not just figuratively, circulate around the world multiple times before the victim even makes it to the police to report the crime. Financial intelligence units are able to identify these networks, but only where it is possible to analyse methods related to money laundering through bank accounts. It is important to establish who has set up the system for laundering funds obtained through fraud, where it has been established, and to which countries and by what means these funds are subsequently transferred.

To track down the organisers of fraud, a more comprehensive approach and analysis of financial data are needed in addition to handling individual cases.

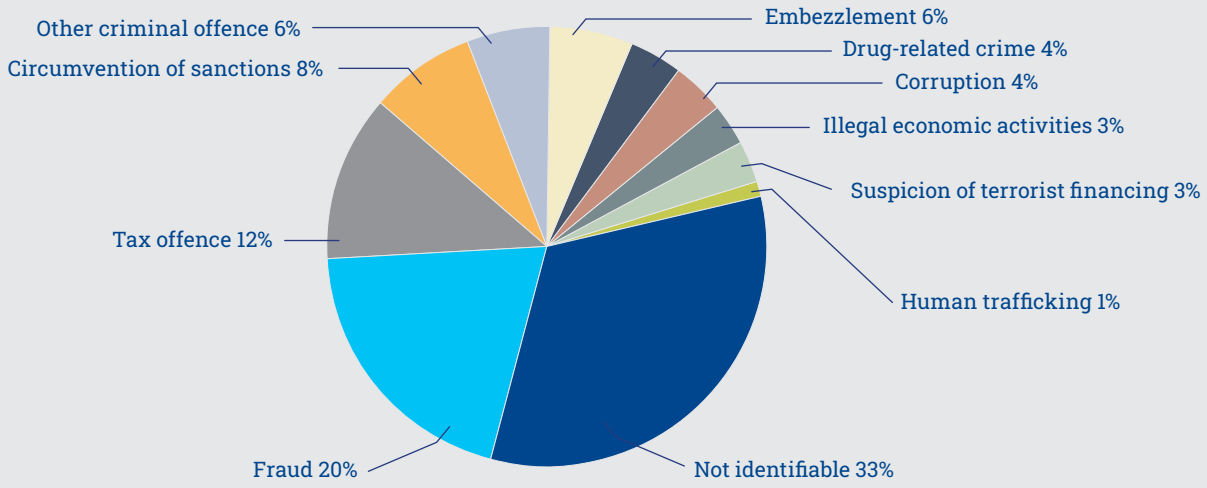
Combating fraud is possible only through co-operation between the public and private sectors – extending beyond obliged entities – and through close international co-operation. While a significant amount of information on fraud is received from Estonian market participants (primarily larger credit institutions) and from abroad, only a small share is sufficiently substantive and suitable for use in proceedings to identify money laundering. It is therefore necessary to find new ways for banks to report even more effectively. In 2025, solutions were explored through the Spinnaker programme for top executives at the Government Office, which resulted in the establishment of a fraud prevention steering group at the Police and Border Guard Board, in which the Financial Intelligence Unit also participates.

The volume of information received by the Financial Intelligence Unit on cases involving suspected **tax offences** and related money laundering has also increased. This reflects the improving ability of obliged entities, particularly credit institutions, to detect tax-related violations through account analysis. In

addition to domestic tax fraud, the number of e-commerce-related fraud cases has also increased. In these schemes, Estonian companies are used to sell goods on European platforms, while the tax obligations associated with the sales are not fulfilled in the country of destination. We also see cases of intra-Community VAT fraud in which Estonian companies are used as buffer entities. Criminal groups, including those operating in foreign countries, have long exploited the ease of establishing companies in Estonia and weak beneficial ownership oversight, making use of these in both tax and other types of crime.

Watch the Financial Intelligence Unit's EFIUC 2025 conference discussion on fraud

Assumed (predicate) offences based on Financial Intelligence Unit case files



MORE VULNERABLE SECTORS

While in mid-2021, there were 641 authorised virtual currency service providers and supervision of the sector was the greatest challenge faced by the FIU, today only 36 service providers operate on the market – a number more in line with the risk profile of a small country. These providers are subject to a regular reporting obligation, which helps to better understand sectoral risks and develop mitigation measures. At the same time, high volumes and non-resident parties continue to make the sector one of the most vulnerable to money laundering.

Payment statistics from credit institutions submitted to Eesti Pank showed a sharp increase (44%) in the volume of cross-border payments in 2025, driven primarily by the business operations of a single bank. Although there has also been a slight increase in the volume of cross-border payments by residents, nearly 99% of the growth is driven by an increase in non-resident transactions,

with payments initiated by other financial institutions standing out in particular. This points to an increased money laundering risk, as it is more difficult to determine the economic substance of transactions, the origin of funds and the beneficial owners of such cross-border transactions.

In 2025, the volume of suspicious transactions reported in connection with suspected money laundering increased significantly. Non-residents account for the majority of suspicious activity reports related to money laundering, although the share of Estonian residents is also increasing among both natural and legal persons.

A separate challenge is the transaction nesting. Five years ago, this topic was discussed mainly in the context of correspondent relationships between credit institutions and this risk remains relevant. Today, new types of nesting can be observed, primarily related to virtual currencies where virtual currency services are provided by virtual currency service providers to other companies in the same sector, to payment intermediaries and to remote gambling service providers. Mitigating risks in services involving layered customer relationships is a challenge for both service providers and supervisors. We also published a separate study on this topic[11].

In the national risk assessment, the gambling sector was rated as having a medium-high risk level. Once again, the Financial Intelligence Unit is facing a challenge similar to that encountered in 2021 with virtual currency service providers. The question is how to supervise remote gambling service providers whose management and operations are based abroad and whose only connection to Estonia is a legal entity registered here. In addition, counterparties to transactions worth billions of euros are often non-residents, sometimes from countries with a very high money laundering risk.

The provision of nested services entails hidden risks that require increased attention from undertakings.

The risk level of company service providers assessed as having medium-high risk is associated with a narrower group of service providers. While virtual currency service providers were previously 'imported', there are now indications that the same risk is also present, among others, in remote gambling service providers. Many service providers still do not understand their role as gatekeepers in preventing money laundering and terrorist financing, nor do they understand the risks associated with the services they offer. The higher risk is also driven by the services provided, such as concealing company directors and beneficial owners and offering fictitious addresses, among others. The results of off-site inspections carried out in 2025 show that, overall, the level of application of due diligence measures and risk awareness in the company service provider sector remains low, although some authorisation holders are making an effort and stand out for their diligence. Several service providers who had not previously understood their role have begun to improve their systems in co-operation with the supervisory authority. We appreciate such open dialogue and believe it helps reduce the overall risk.

MONEY LAUNDERING METHODS AND TYPOLOGIES

The issue of money laundering as a service, ie professional money launderers, has gained increasing international attention in recent years, including the specialisation of providers of such services (providers of 'solutions' related to crypto-assets, schemes linked to online casinos etc). In recent years, the attention of the Financial Intelligence Unit has been drawn to several cases in which Estonian persons or non-residents have provided money laundering services through Estonian service providers or participated in international networks offering such services. In this yearbook, we will present one conviction in this area.

Shell companies and straw persons, fictitious transactions, counterfeit invoices and contracts, as well as virtual currencies and trade- and service-based money laundering continue to be used for money laundering purposes. Cases were also identified in which the transaction laundering typology was used to conceal and legitimise criminal proceeds.

'Transaction laundering' means the execution of prohibited or concealed transactions through an ostensibly legitimate merchant or payment channel in order to conceal the true nature or origin of the transactions. For example, card transactions are subject to mandatory merchant category coding, which enables monitoring of the types of transactions being processed. Such coding makes it possible to block transactions that are illegal in certain countries. In this way, companies can deceive payment service providers by, for example, classifying gambling payments as transactions involving the purchase and sale of commercial photographs, thereby enabling gamblers to use services provided by operators that do not hold the required authorisation in their country of residence.

An increasing number of cases were also identified in which salary or dividend payments that did not reflect reality were made to persons in order to conceal and legitimise criminal assets. In some cases, taxes were also declared on these payments to further conceal their true nature. There was also an increase in suspicious transactions in remote gambling.

Although the market for virtual currency service providers in Estonia has now been regulated, cryptocurrency remains an important tool for laundering criminal proceeds. This is not so much due to the suspicious activity by Estonian market participants themselves, but rather due to the inherent money laundering risks associated with virtual currencies and the weak measures in place for identity verification, customer relationship monitoring and monitoring of suspicious transactions. Therefore, the analysis of money laundering risks

associated with the use of virtual currencies will remain the responsibility of the Financial Intelligence Unit and a priority in the foreseeable future even after July 2026 when the Financial Supervision Authority begins supervising crypto-asset service providers.

As a centre for risk analysis, the Financial Intelligence Unit will continue to focus in the coming years on higher-risk areas, using the most intelligent and digitally advanced solutions available. The aim is to be a strong partner for both the private sector and state agencies in Estonia and abroad, and to protect our economic environment and financial system.

Watch an explanatory video on money laundering and terrorist financing (in Estonian)

REPORTING

In 2025,

14 323

reports were filed,

incl

10 443

suspicious transaction or unusual transaction reports

The number of reports remained at the same level as in 2024 and, over the past five years, a moderate downward trend has been observed.

Credit institutions stand out for above-average reporting activity and report quality. Thirteen of the 14 credit institutions submitted reports accounting for more than 40% of all reports. A total of 60% of virtual currency service providers reported to the Financial Intelligence Unit, which is a significant step forward. However, the reports primarily concerned suspicions of money laundering that arose during the conclusion of contracts with customers, rather than activities indicative of money laundering typologies.

In the gambling operators sector, reports were received from 40% of market participants. In several sectors, reporting activity remains extremely low: only 6% of company service providers and less than one tenth of financial institutions submitted reports.

Across all sectors, the main shortcoming in reporting is the delay in identifying suspected money laundering. This means that by the time the report is submitted, money laundering has already taken place and the proceeds of criminal activity have been transferred, making interception no longer possible.

Market participants can improve the quality of reports in two ways: by providing more detailed explanations of the grounds and content of suspicions, and by correctly completing transaction and other data fields.

BREAKDOWN OF REPORTS								
	Suspicious transaction report (STR)	Unusual activity report (UAR)	Unusual transaction report (UTR)	Terrorist financing report (TFR)	International sanctions report (ISR)	Inquiry	Cash transaction report (CTR)	Total
Credit institution	4048	1122	281	33	271			5755
Virtual currency service provider	2443	184	147	44	92			2910
Financial institution	1152	252	108	51	12	1	1033	2609
Gambling operator	129	60	38				1366	1593
Foreign entities and persons	20	6			37	587	1	651
Professionals (legal services, audit, etc)	56	39	106	7	15		131	354
Other private operators	37	1	18		3		119	178
Not an obliged entity	113	23	4	1	12		7	160
State agency	37	9	10	2	13	33	9	113
Total	8035	1696	712	138	455	621	2666	14323

The Financial Intelligence Unit uses all reports in both strategic and tactical analyses. In addition, some reports are also used for in-depth analysis. Therefore, it is important that all submitted reports are in a valid form and that the fields for transaction details, parties and other information are properly completed.

Some strong reports submitted by market participants on suspicions of money laundering were not included among the candidates for the best report, as the assets had already been moved by the time the report was submitted. The best report was a report by a virtual currency service provider on suspicion of terrorist financing. The 2025 best report is therefore described in more detail in the chapter on terrorist financing.

The Financial Intelligence Unit contributes to improving the quality of reports in several ways: by providing feedback to sectors through public reports and

PLEASE NOTE

When describing transactions in a report, the FIU recommends using a structured narrative, addressing the following questions: what, who, when, where, why and how.

It is important that reports reach the Financial Intelligence Unit in a timely manner. If suspicious activity is detected late and reported only afterwards, the authority's options for operational intervention may already have been exhausted.

directly to credit institutions, as well as through bilateral meetings, training sessions, information and video materials. In 2025, alongside the EFIUC 2025 conference, the FIU organised a **simulation exercise** in which partners from the private sector and state agencies carried out their regular duties in a simulated environment. Over three days, 82 people participated in the exercise, including representatives of virtual currency and company service providers, notaries, banking specialists, analysts from the Financial Intelligence Unit, as well as investigators and prosecutors.

Internationally recognised expert and consultant Yehuda Shaffer, together with the Head of the Financial Intelligence Unit Matis Mäeker, Deputy Head Markko Kard and several FIU staff members, advised and guided representatives of the private sector. The analysts of the Estonian FIU were, in turn, guided by the heads of the FIUs of the Netherlands and Latvia. Representatives of investigative authorities were additionally instructed by State Prosecutor Alar Lehesmets.

As a result of the training, the FIU gained a good overview of how market participants approached the analysis of money laundering cases, including their reasoning, knowledge, capabilities and methods used. The discussions between investigators and prosecutors also provided valuable input that can be used in future analyses and disclosures.

DEVELOPMENT OF A NEW INFORMATION SYSTEM

In 2024, the Financial Intelligence Unit began developing a new information system. The goal was to improve the overall quality of reports, including making the reporting process more user-friendly, organising the information more effectively and providing better feedback to reporting entities. Over the course of two years, an analysis has been conducted, a new system has been implemented in the development environment and an updated report form has been developed.

In 2026, development will continue, including planned testing with market participants, the release of documentation necessary for X-tee development, the preparation of guidelines and the updating of regulations. The new information system is scheduled to be launched in early 2027.

SIMULATION EXERCISE AT THE FINANCIAL INTELLIGENCE UNIT'S EFIUC 2025 CONFERENCE

The Financial Intelligence Unit developed a case study based on real cases, including example evidence. These concerned an international money laundering scheme in which persons operating in different jurisdictions established and used shell companies to ostensibly launder assets obtained through criminal activity. To conceal traces, transactions were also carried out in crypto-assets and funds derived from criminal activity were integrated into real estate.

On the first day of training, representatives of company service providers, virtual currency service providers, notaries and banks were given a tip regarding a suspicious transaction: an Estonian company received 1.2 million euros that did not match the customer profile.

- Participants asked the facilitators of the FIU for additional information that they would normally be able to request from the customer and obtain from their own databases, different registers and public sources.
- A transaction with high-risk indicators was analysed, which had to be placed in a broader context and the suspicious circumstances related to the case identified.
- A notary submitted a report to the Financial Intelligence Unit, noting that the time pressure to complete the transaction quickly and the fact that the buyer's representative does not reside permanently in Estonia raised suspicions.
- A company service provider emphasised in its report to the Financial Intelligence Unit that the establishment of two Estonian companies was paid for by a third party – a company registered abroad.
- Reports from banks indicated incomplete customer information forms and that the origin of funds had been obscured through multiple jurisdictions, legal entities and complex transaction chains.
- Virtual currency service providers identified the use of different crypto-asset wallets.

On the second day of the training, the FIU analysts received the reports prepared on the previous day.

- The reports were analysed.
- In addition to evidence from the private sector, supplementary material was collected to verify suspicions and identify additional circumstances and links.

- The analysts asked the facilitators for information that, in a real-life situation, could have been obtained from different national registers, restricted-access databases, foreign partners and the blockchain.
- A disclosure was prepared for the investigative authority, describing the suspicion of money laundering, the circumstances indicating it and relevant typologies, as well as the possible role of natural and legal persons.

On the third day of the training, the disclosure of the Financial Intelligence Unit reached the investigators and prosecutors.

- The disclosure was analysed.
- Criminal proceedings were initiated. During the proceedings, additional evidence prepared by the facilitators was collected through register inquiries, letters rogatory, searches and the questioning of witnesses and suspects, as well as through a number of other procedural acts.
- Based on the disclosure of the Financial Intelligence Unit and the additional evidence gathered through procedural acts, the investigators and prosecutors decided which persons to charge and which facts and evidence support the charges.
- Charges were filed against different natural and legal persons. The necessary elements of the criminal offence included the following identified instances: provision of money laundering as a service, acquisition of criminal assets, transformation and concealment of criminal proceeds, falsification of documents and the knowing use of falsified documents, activities without authorisation. Charges were also brought against professionals who failed to adequately fulfil their due diligence obligations, thereby contributing to money laundering.



CO-OPERATION IN THE PREVENTION OF MONEY LAUNDERING

In 2025,

147
analysed disclosures were filed with investigative authorities concerning 311 reports

1109
disclosures were filed with investigative authorities concerning 2,058 reports and cross-border information

232
foreign inquiries and spontaneous disclosures were filed

589
foreign inquiries and spontaneous disclosures were received

The task of the Financial Intelligence Unit is to analyse the information received from reports and, if suspicion persists, to disclose the information to investigative authorities. In 2025, the following were filed:

- **116** disclosures regarding money laundering and suspicions of such an offence. Compared to the previous year, the volume of case studies and disclosures remained the same;
- **17** disclosures regarding violation of international sanctions;
- **8** disclosures regarding terrorist financing;
- **3** disclosures or crime reports based on authorisation and supervisory proceedings.

Information was disclosed to investigative authorities mainly on suspicions of money laundering or aiding money laundering, as well as on suspicions of fraud, embezzlement, corruption, tax and drug-related offences, sanctions evasion and economic activities without authorisation, which were related, among other things, to the granting of credit and the provision of virtual currency and company services. Compared to 2024, the number of cases involving suspicion of economic activities without authorisation increased.

Based on information disclosed by the Financial Intelligence Unit, 15 criminal proceedings were initiated (10 criminal cases in 2024). Criminal proceedings were initiated on multiple elements of a criminal offence: money laundering, including sanctions violations, economic activities without authorisation, embezzlement, benefit fraud, tax offences, and requesting access to child pornography and watching thereof.

According to investigative authorities, 75% of the disclosures made by the Financial Intelligence Unit contained information that was new to them and, in most cases, this information was valuable for intelligence gathering and analysis. Nearly one quarter of the information disclosed to investigative authorities was valuable for initiating or conducting criminal proceedings.

Timely reports from obliged entities and financial information disclosed by the Financial Intelligence Unit have proven valuable to investigative authorities in 75% of cases.

ANALYSIS FOLLOWING THE REPORT AND PRECEDING CRIMINAL PROCEEDINGS, WHICH ESTABLISHED THE SUSPICION

Established circumstances:

- The Financial Intelligence Unit received reports from market participants indicating that ship brokerage transactions were identified on the bank accounts of N OÜ, but the economic rationale was unclear. Suspicions arose that the transactions were fictitious and that their purpose was to channel funds obtained through criminal activity, which had been laundered through banks, into real estate under the name of A, partner of the owner of N OÜ.

Verification of suspicion of money laundering:

- The Financial Intelligence Unit developed a suspicion that money laundering had been committed. Several million euros of funds of unclear origin were transferred to the bank account of N OÜ from a third-country company B and from an EU-registered company NA, which was part of the Russian Holding Group. The initial hypothesis was that N OÜ and its owner S had embezzled funds from company NA and had engaged in money laundering of funds derived from criminal activity. The information received by the FIU in the report included the bank accounts of N OÜ, certain companies associated with S, and S. Given this limited information, the investigative authorities, in co-operation with the Prosecutor's Office, are unable to initiate criminal proceedings, as there is insufficient information regarding the possible criminal offence and the suspicion thereof. Furthermore, the circumstances indicated in the report are not sufficient to meet the threshold for initiating criminal proceedings for money laundering.
- For this reason, the Financial Intelligence Unit exercised its authority under the Money Laundering and Terrorist Financing Prevention Act (MLTFPA), EU legislation and international standards to verify the suspicion of money laundering and, where possible, to secure the funds. To verify the suspicion of money laundering, it was necessary to identify the movement of funds derived from possible criminal activity among the persons involved in the suspicion. Justified requests

were made to credit institutions Y and C to obtain bank account statements for the following persons:

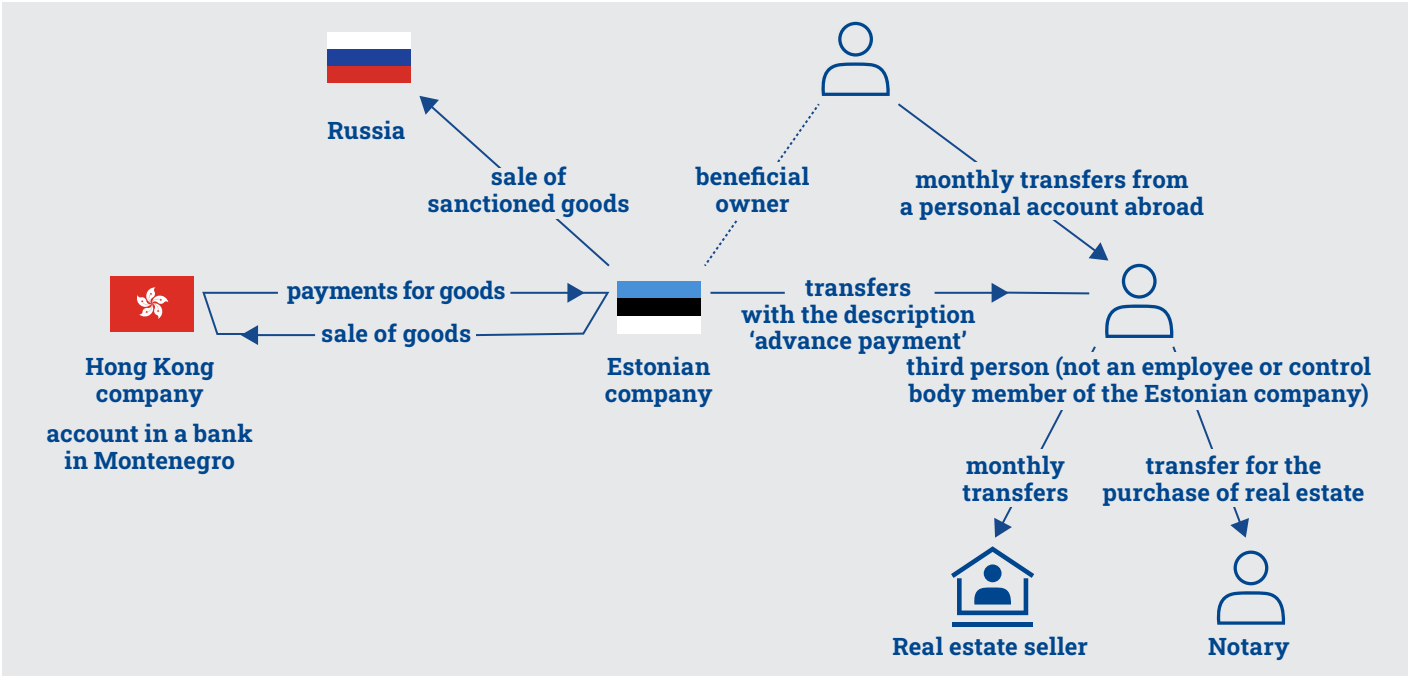
i) person A suspected of being a straw person (to whom N OÜ transferred a registered immovable);

ii) person S and other companies associated with S to whose accounts N OÜ made transfers.

- Additional account data showed that person S transferred funds to the account of person A in round amounts, which is indicative of money laundering typologies. In part, the transferred funds originated from several companies associated with S, one of which was H OÜ. The descriptions of the transfers made by companies to S were generic, eg 'to cover economic expenses' or 'advance payment', which is also indicative of money laundering typologies. In addition to the above, the bank account of A revealed that A received a total of nearly 50,000 euros in four instalments from H OÜ, described as 'advance payment'. The funds received from H OÜ were used to pay the notary for the registered immovable.
- Further inquiries revealed that person A was neither an employee of H OÜ nor a member of its management board or a shareholder, which made such a transfer of funds unusual. The circumstances surrounding the sale of the registered immovable were unusual because the income of person A would not, under normal circumstances, have been sufficient to purchase such real estate.

Verification of additional suspicions:

- Based on the foregoing, suspicions arose that the assets of N OÜ were intended to be transferred or registered in the name of A, where A was in reality a straw man who held the funds on behalf of N OÜ and its owner without being the beneficial owner. In this way, the true ownership of the assets was concealed.
- Therefore, the Financial Intelligence Unit made a justified request for the bank accounts of H OÜ in order to determine the origin of the funds transferred to person A for the purchase of the real estate.
- The request revealed that the funds on the account of H OÜ, part of which were transferred to person A, originated from a third-country company M, which held an account with a bank registered in the EU. M transferred funds to H OÜ four times in the total amount of more than 650,000 euros with the description 'sale of XXXX'. XXXX was a sanctioned good.
- • Further inquiries revealed that the sanctioned goods sold by H OÜ to the third-country company were shipped to Russia after the final payment was made and were registered in the Russian register.



Summary:

The initial suspicion of money laundering reported by the banks was not confirmed, but during its verification, the Financial Intelligence Unit determined that the company H OÜ covertly sold sanctioned goods through third parties to a Russian company and derived criminal proceeds from the sale of those goods, meaning that the necessary elements of the offence set out in § 931 of the Penal Code were present. The funds derived from international sanctions violation were transferred to the bank account of private person A, who exhibited characters of a straw person, and were used to finance the real estate transaction. Consequently, there were grounds to believe that H OÜ, its representative S and person A had committed or participated in money laundering (§ 394 of the Penal Code). The objects of money laundering constituted the funds transferred from the bank account of H OÜ to A, which were derived from a sanctions violation. The suspicious transactions of H OÜ took place on an account opened with bank Y in Estonia, regarding which the bank did not submit a report. Likewise, bank C did not submit a report regarding the suspicious transactions on person A's account.

In this case, further identification of activities suspected of money laundering was only possible through requesting additional account data and subsequent analysis. An analyst at the Financial Intelligence Unit began analysing the suspicion based on information contained in a report submitted by a notary. As a result of the analysis, the FIU disclosed to the investigative authority a suspicion of a violation of international sanctions and the concealment of proceeds derived therefrom, and criminal proceedings were initiated.

Watch the Chief Public Prosecutor's presentation on money laundering investigations at the Financial Intelligence Unit's EFIUC 2025 conference (in Estonian)

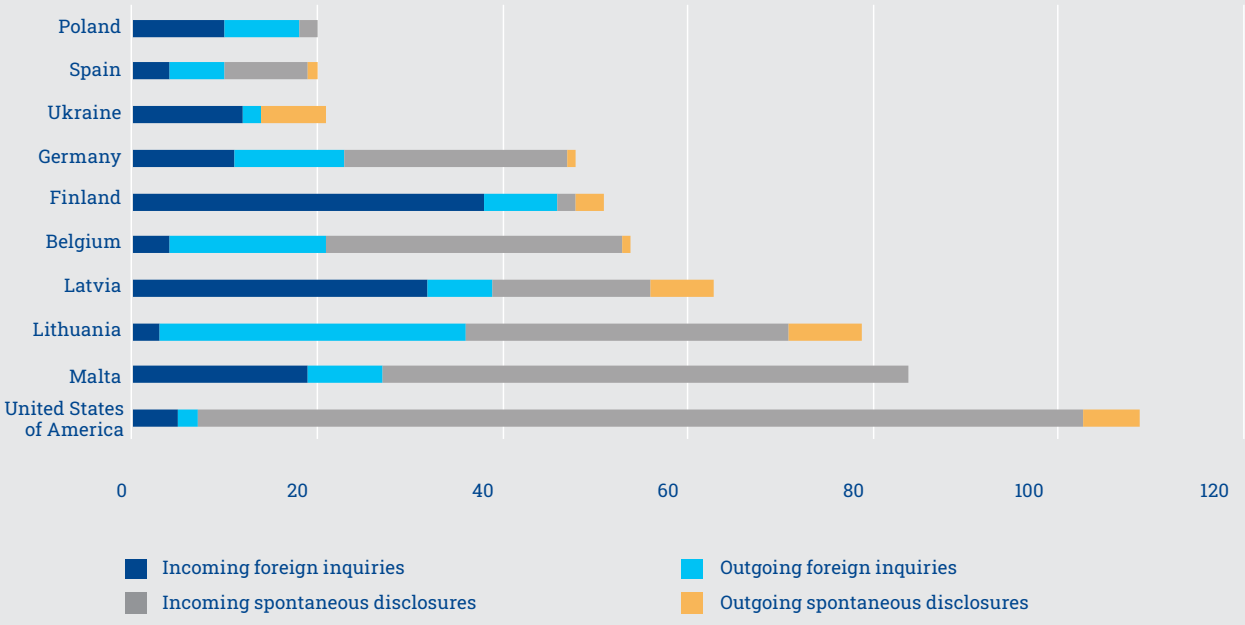
Inquiries and information exchanges with foreign financial intelligence units confirm the trend that funds suspected of money laundering are increasingly being transferred abroad and/or to Estonia from foreign countries.

The highest number of inquiries and information exchanges were made with Lithuania, followed by Belgium and Germany. This, in turn, illustrates where persons linked to Estonia hold accounts or assets and where funds suspected of money laundering were transferred.

The Financial Intelligence Unit received the most inquiries from Finland, Latvia and Malta. These inquiries revealed that funds derived from fraud had been deposited into the accounts of Estonian companies and persons, and that Estonian companies were linked to tax fraud committed in foreign countries. Companies established in Estonia continue to be used in criminal activities abroad. For example, there has been an increase in cases where Estonian companies are used to sell goods on e-commerce platforms to conceal the tax liability arising from such sales.

Inquiries from foreign financial intelligence units continue to indicate the misuse of Estonian companies in criminal schemes.

The financial intelligence units that have co-operated the most in the fields of money laundering, terrorist financing and financial sanctions in 2025



Watch the presentation by the Head of the Dutch FIU on the detection of money laundering offences at the EFIUC 2025 conference

In strategic co-operation, contributions were made to ongoing global and regional forms of co-operation. Although the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) is planned to achieve full operational capacity by 2028, preparatory work already gained momentum last year – meetings of the General Board were held and the FIU provided feedback on procedural proposals as well as on guidelines and other documentation.

The General Board of AMLA comprises:

- an FIU composition, of which the member from Estonia is the Head of the Financial Intelligence Unit;
- a supervisory composition, of which the principal member from Estonia is a Member of the Management Board of the Financial Supervision Authority, and the alternate member is the Deputy Head of the Financial Intelligence Unit.

In the coming years, market participants can expect several regulatory and implementing technical standards to be introduced, first to provide feedback to AMLA and then to integrate them into their operations. Providing feedback makes it possible to influence future requirements before they enter into force; once in force, they will apply across the European Economic Area, directly affecting Estonian market participants as well. The FIU publishes on its website calls for feedback on technical standards and information on their adoption.

5 YEARS

Feedback from foreign countries indicates that the Financial Intelligence Unit continues to have a strong international reputation in both operational and strategic co-operation. The FIU contributes through active participation in the work of international organisations, responds promptly to foreign inquiries and shares its analyses with the international community or conducts them in co-operation with partner countries. However, the restriction to accessing bank accounts may significantly harm international co-operation. FIUs operate on the principle that if one FIU applies restrictions, the other does the same.

The FIU shares English-language updates for the international community on the LinkedIn account of the Estonian Financial Intelligence Unit (FIU).

Watch the discussion on the ongoing MONEYVAL sixth evaluation round at the Financial Intelligence Unit's EFIUC 2025 conference

DISPOSAL RESTRICTIONS AND ADMINISTRATIVE CONFISCATION

30-day restrictions were imposed in 6 cases on approximately **124,000 euros,** including 2 cases related to terrorist financing in virtual currencies

60-day restrictions were imposed in 2 cases on approximately **14,000 euros**

365-day restrictions were not imposed

3 compliance notices were issued ordering the transfer of **18,200 euros** to state revenue

In criminal proceedings, previously restricted assets were attached in 6 cases, totalling **1.24 million euros**

Significantly fewer disposal restrictions were imposed than in 2024, when assets were restricted in several cases, different restrictions were imposed and the volume of restricted assets was higher. The volume of disposal restrictions in 2025 was influenced not only by diverse money laundering cases but also by case law, as well as by the fact that the Financial Intelligence Unit did not receive sufficiently high-quality information in a timely manner. This means that by the time the assets were restricted, the assets were no longer in the account, as the potential money laundering was detected too late. The 18,200 euros transferred to state revenue with the authorisation of the court were related to a case described in greater detail in the 2023 Yearbook, in which an attempt was made in Estonia to exchange banknotes originating from Libya.

In 2024, following initial work by the Financial Intelligence Unit, investigative authorities attached assets subject to seven disposal restrictions in criminal proceedings, with a total value of 5.4 million euros. In 2025, assets subject to six restrictions were attached, totalling 1.24 million euros.

PLEASE NOTE

Obligated entities must identify suspicious transactions in a timely manner and promptly notify the Financial Intelligence Unit. In several cases, transactions suspected of money laundering were carried out, funds were transferred out of the account and only then were the transactions/customer inspected, the suspicion identified and a report submitted. In such cases, the Financial Intelligence Unit is unfortunately only able to impose a restriction on the account balance, provided that funds are still available on the account.

AN IMPORTANT COURT DECISION CONCERNING THE RIGHT TO IMPOSE RESTRICTIONS

- Administrative case 3-21-2882 concerned contestation of the lawfulness of compliance notices issued by the Financial Intelligence Unit, under which a disposal restriction was imposed on the 750,000 euros held in the person's bank account, initially for 30 days and subsequently for 60 days.
- The Financial Intelligence Unit suspected that the person was using their spouse and the company registered in their name to transfer funds derived from the person's own possible criminal activities to France via the complainant's bank account in Estonia. In order to disrupt possible criminal activity, preserve existing assets and establish further circumstances related to the origin of the funds, the Financial Intelligence Unit imposed a disposal restriction. The funds that gave rise to suspicion had been deposited to the bank account of the complainant through different channels, including through different jurisdictions over a short period of time (Russia–Estonia–Liechtenstein–Estonia), and were intended to be further transferred to France for the purchase of real estate. The use of multiple jurisdictions to move funds is a money laundering typology employed to conceal the true origin of funds and reduce the likelihood that local credit institutions will detect unusual transactions. Real estate transactions, in particular, are frequently used to commit international money laundering and, according to the European Union-wide risk assessment, real estate acquired for investment purposes poses the highest risk of money laundering.
- In its decision of 4 July 2025, the circuit court of appeal found that
  - the compliance notices issued by the Financial Intelligence Unit were lawful;
  - the question of whether assets suspected of money laundering originate from criminal activity is ultimately determined in criminal proceedings. The Financial Intelligence Unit does not decide whether money laundering or terrorist financing has taken place;
  - the lawfulness of administrative acts is not retrospectively affected by the fact that, on the basis of an application by the Financial Intelligence Unit, criminal proceedings were initiated against the complainant in connection with the case in question pursuant to clause 3 of subsection 2 of § 394 of the Penal Code (money laundering on a large-scale basis), but were later terminated due to lack of grounds. The circuit court of appeal noted that the initiation of criminal proceedings and the attachment of assets to ensure confiscation indicated that the suspicion held by the Financial Intelligence Unit was still sufficient and justified in February 2022. There is no basis for the argument that the suspicion of money laundering was sufficient for the attachment of the complainant's assets in criminal proceedings, but insufficient to impose a disposal restriction on them on the basis of compliance notices issued by the Financial Intelligence Unit.

ADMINISTRATIVE CONFISCATION

In the 2024 Yearbook, we covered a case involving two Estonian citizens in the United States, where the individuals pleaded guilty to participating in a criminal conspiracy to commit fraud. Within the framework of the agreement reached, the defendants assigned to the United States a large portion of their personal assets, valued at more than 400 million US dollars, according to a press release by the US Department of Justice[2]. The court in Seattle sentenced the accused to community service under the supervision of a probation worker and also imposed a fine of 25,000 US dollars on each of them.

By a decision of the Supreme Court dated 31 March 2025, the request of the Financial Intelligence Unit for authorisation to transfer the restricted assets to state revenue was dismissed, as not all the conditions for administrative confiscation had been met. The Supreme Court emphasised in its decision that, in the case of self-laundering, which was the basis of the suspicion, administrative confiscation is likely not possible, as the civil-law and economic owner of the assets (the beneficial owner) coincide. Therefore, the Supreme Court found that in this case the owner and beneficial owner of the assets were known, thus administrative confiscation of the assets was not permissible, regardless of the fact that the other conditions had been met. These assets did not include the assets attached in the criminal proceedings taking place in the United States.

The Supreme Court defined the grounds for administrative confiscation, which may be relied upon in future cases.

SUPREME COURT DECISION CLARIFYING THE PERMISSIBILITY OF ADMINISTRATIVE CONFISCATION

On 12 June 2025, in its decision in administrative case 3-24-1840, the Supreme Court granted the request for authorisation of the Financial Intelligence Unit and further clarified the conditions for the permissibility of administrative confiscation, which were set out in the decision of the Supreme Court of 31 March 2025:

1) When deciding whether to grant authorisation for administrative confiscation, the administrative court must first determine, under the current law, whether there is a good reason why the assets cannot be confiscated in criminal proceedings (the principle of subsidiarity). Such good reasons may include the lapsing of the limitation period for the offence, terminal illness or death of the suspect or accused, evasion of criminal proceedings or immunity, termination of criminal proceedings due to evidentiary challenges (in particular the impossibility of international co-operation), criminal proceedings conducted in another country and the resulting need to avoid a breach of the *ne bis in idem* principle etc.

2) As regards the other conditions required for administrative confiscation, the administrative court may limit itself to assessing whether the transfer of the assets to state ownership is not manifestly precluded. These other conditions are as follows (cumulatively):

- the request was submitted by the Financial Intelligence Unit or the Prosecutor's Office;

- one year has lapsed since the imposition of restriction on the disposal of assets;

- the disputed assets remain linked to suspected money laundering (subsection 1 of § 57 of the MLTFPA) and the legal origin of the assets has not been proven (clause 1 of subsection 3 and subsection 10 of § 57 of the MLTFPA). This condition requires an assessment of the following circumstances: (a) the existence of a suspicion of money laundering; (b) the continuing nature of the suspected money laundering; (c) the suspicion relates to the disputed assets; and (d) the legal origin of the assets has not been proven, ie the link between the assets and the suspicion of money laundering has not been rebutted. The Financial Intelligence Unit must prove that money laundering occurred on the balance of probabilities. The person has the opportunity to provide reasons demonstrating that the assets (or part thereof) are of legal origin, ie rebut the suspicion of the Financial Intelligence Unit that the assets are of criminal origin at least to the extent that the suspicion regarding the legality of the assets is no longer sufficient to meet the balance of probabilities;

- it has not been possible to identify the owner of the assets, the beneficial owner (or owner) of the assets held on the account or the possessor of the assets has expressed a desire to give up the property.

The Supreme Court added that the order in which the conditions are examined is irrelevant. The assessment may begin with the question of whether the transfer of assets to state ownership is subsidiary or with whether administrative confiscation is manifestly precluded, having regard to the conditions set out in subsection 7 of § 57 of the MLTFPA.

In the present case, in which the request for authorisation was granted, the Supreme Court found that the Financial Intelligence Unit had reasonably and plausibly substantiated the existence of a continuing suspicion of money laundering, based on the balance of probabilities, in respect of all the disputed assets. Furthermore, the person concerned failed to rebut the suspicion of the FIU regarding the legal origin of the assets. The court added that identification of the owner of the account assets does not preclude the administrative confiscation of the account assets if the court is satisfied that the beneficial owner remains unidentified. This was precisely the situation in the present case. As regards the impossibility of conducting

criminal proceedings, the court found, based on the explanations provided by the Financial Intelligence Unit, that the condition of subsidiarity for the application of administrative confiscation was also satisfied in this case.

In light of the foregoing, the Supreme Court granted the interim appeal of the Financial Intelligence Unit and upheld the order of the Tallinn Administrative Court, which granted authorisation to transfer to state ownership assets amounting to 74,376.44 euros that had been subject to restrictions imposed by the FIU and related to a suspicion of money laundering.

The 18 new litigation cases initiated in 2025 – some of which were later consolidated – concerned the following:

- contestation of compliance notices issued by the Financial Intelligence Unit requiring obliged entities to provide additional information;
- decisions of the Financial Intelligence Unit imposing access restrictions on requested information and refusing to disclose information;
- a claim seeking annulment of a single order to pay a non-compliance levy;
- in one case, a request to oblige the Financial Intelligence Unit to issue a statement refuting the inaccurate claims made in an article;
- authorisations in three cases.

Approximately 85% of court decisions which have entered into force over the past five years have resulted in a positive outcome for the Financial Intelligence Unit. If the consequences of the judgment of the Supreme Court of 31 March 2025 on administrative confiscation are excluded, where more than 30 parallel court proceedings were ongoing in the same case involving the same persons (for the administrative confiscation of each asset, four administrative acts can be challenged: the 30-day, 60-day and one-year restrictions and the decision to transfer to state revenue), the proportion of favourable court decisions is even higher.

Watch the Financial Intelligence Unit's EFIUC 2025 conference discussion on non-conviction-based confiscation

MONEY LAUNDERING CONVICTIONS

In 2025, three district court judgments and two circuit court of appeal judgments entered into force in Estonia, resulting in six convictions and two acquittals. The court resolved three cases through a plea agreement procedure and two cases under regular rules of procedure.

All six convicted persons were sentenced to imprisonment, the enforcement of which was suspended for four of the accused and, for one accused, the court substituted imprisonment with community service. Based on court judgments, assets with a total value of more than 65,000 euros and, in one case, the right of claim in respect of shares were confiscated.

At the beginning of 2025, a judgment of the circuit court of appeal in case 1-20-3487 entered into force, by which the court found Andrii Danchak, a member of the management board of GFC Good Finance Company AS (GFC), guilty of aiding money laundering and acquitted two persons of money laundering charges. The case was initiated on the basis of a criminal report by the Financial Intelligence Unit and was described in more detail in the 2024 Yearbook.

By the decision No 1-24-4430 of the Tartu Court of Appeal of 11 April 2025, the first persons – Igor Bogovski and Irina Bogovskaia – were found guilty of laundering cash stolen from Ukraine. In both 2023 and 2024, the yearbooks of the Financial Intelligence Unit have highlighted a suspicion of a criminal offence in which cash stolen from Ukraine, or otherwise derived from criminal offences committed there, was attempted to be transported through Estonia. In several cases, the cash that was discovered and seized could be confiscated and transferred to state revenue by court authorisation granted at the request of the Financial Intelligence Unit. In the assessment of the court, the persons committed money laundering in a group and on a large-scale basis, ie a criminal offence pursuant to clauses 1 and 3 of subsection 2 of § 394 of the Penal Code. They transported hryvnias as couriers from Finland through Estonia, Latvia and Lithuania to Poland. In addition, they laundered hryvnias through currency exchange transactions, cash payments and the purchase of goods.

In several cases over the years, on the basis of court authorisations requested by the Financial Intelligence Unit, it has been possible to have cash suspected of having been illegally derived from Ukraine transferred to state revenue.

In 2025, another business email compromise (BEC) fraud case was concluded at the Harju District Court under the plea agreement procedure. In court case 1-25-2071, Tigran Šachparonian was charged under clauses 1 and 3 of subsection 2 of § 394 of the Penal Code with money laundering committed in a group with A. V. (deceased) and on a large-scale basis, within the meaning of § 12^1 of the Penal Code. The total amount of money laundered on a continuous basis was 248,531.32 euros.

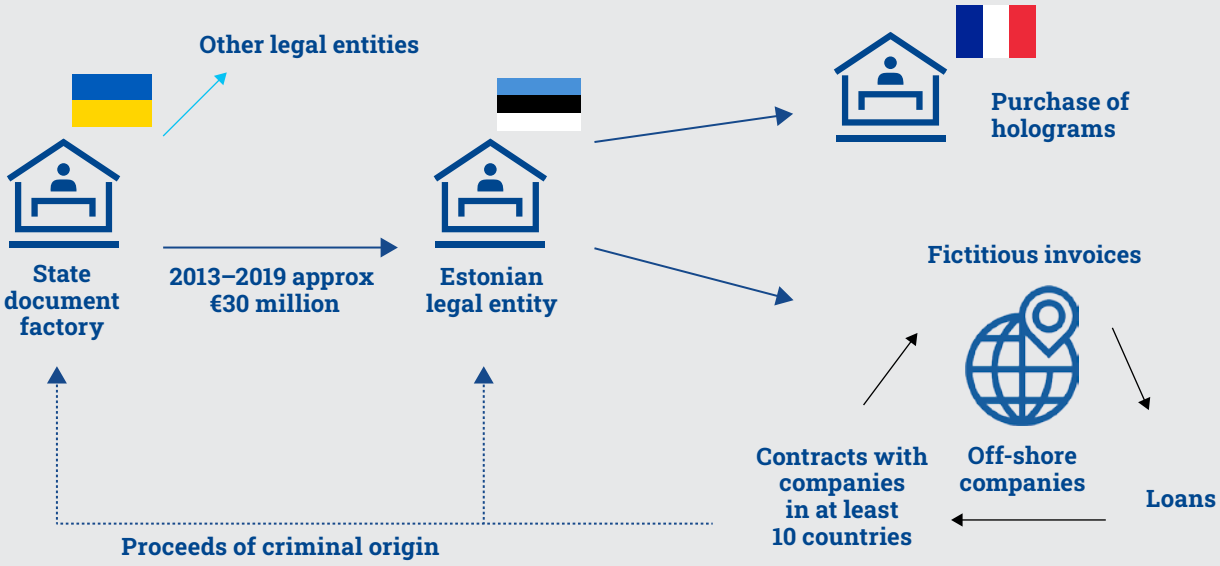
On 15 May 2025, Harju District Court entered a judgment of conviction under plea agreement procedure in court case 1-25-1632 concerning the provision of money laundering as a service. From October 2022 to 19 August 2024, Anton Prektold provided money laundering services to unidentified persons, which consisted of making bank transfers in exchange for an agreed-upon percentage, ie fee, of the laundered amount, with the aim of concealing the true origin of the funds and the beneficial owner. Aleksander Vainik aided in the commission of the offence. To provide money laundering services, Prektold recruited hitherto unidentified natural persons, identified different legal persons and bank accounts through which he could make bank transfers to conceal the true origin and beneficial owner of funds entrusted to him for laundering. The Financial Intelligence Unit supported the police in conducting the proceedings and analysed suspicions of money laundering related to cryptocurrency transactions.

On 28 October 2025, a plea agreement was reached with the accused in case 1-25-5508 concerning a Ukrainian document factory. This case is a notable example of how detailed and time-consuming the detection of money laundering schemes can be, the extent to which it depends on the attention and engagement of different stakeholders, and how this may lead to the late detection of such schemes. We referenced this case in the 2021 FIU Yearbook in connection with cross-border co-operation in uncovering the scheme. We are now presenting it in full.

LAUNDERING OF MONEY ORIGINATING FROM A UKRAINIAN DOCUMENT FACTORY

- Between 2013 and 2019, alongside other companies, nearly 30 million euros were transferred from the Ukrainian State Document Factory to the account of an Estonian company.
- Part of the money was used to purchase holograms from France, while the remainder was funnelled into a money laundering scheme. Off-shore companies were involved in the scheme and fictitious invoices, loans and contracts were exchanged with companies in at least 10 countries.
- Based on international communications with the Financial Intelligence Unit that began in 2018, the parties and circumstances related to criminal proceedings initiated in a foreign country in 2019 were identified.
- In May 2020, the Financial Intelligence Unit opened a case file to continue the analysis of the matter to identify related legal and natural persons, transaction partners, suspicious transactions, other relevant management board members, owners and beneficial owners.
- In October 2020, the police initiated criminal proceedings on suspicion of money laundering based on information provided by the Financial Intelligence Unit.

- Aivar Riis and persons X and Y were charged with money laundering on a large-scale basis with the assistance of person C, in the course of which they knowingly helped conceal the funds derived from a criminal offence committed in Ukraine. According to the charges, the laundered money originated from embezzlement committed by public officials, ie misuse of official position, at a Ukrainian public undertaking. Between 2013 and 2021, the persons provided a money laundering service in Tallinn for a fee, channelling funds derived from criminal activity into the legal economic and financial system of Estonia. In the course of this activity, a number of transactions and transfers were carried out with the aim of concealing both the illicit origin of the funds and their beneficial owners, and all parties were aware that the funds at their disposal originated from criminal activity.
- The court found Aivar Riis guilty of committing the offence specified in clauses 1 and 3 of subsection 2 of § 394 of the Penal Code and imposed a sentence of four years' imprisonment, which will not be enforced if he does not commit a new intentional criminal offence within a period of probation of 4 years and 6 months.
- Proceedings against the other accused persons are ongoing.

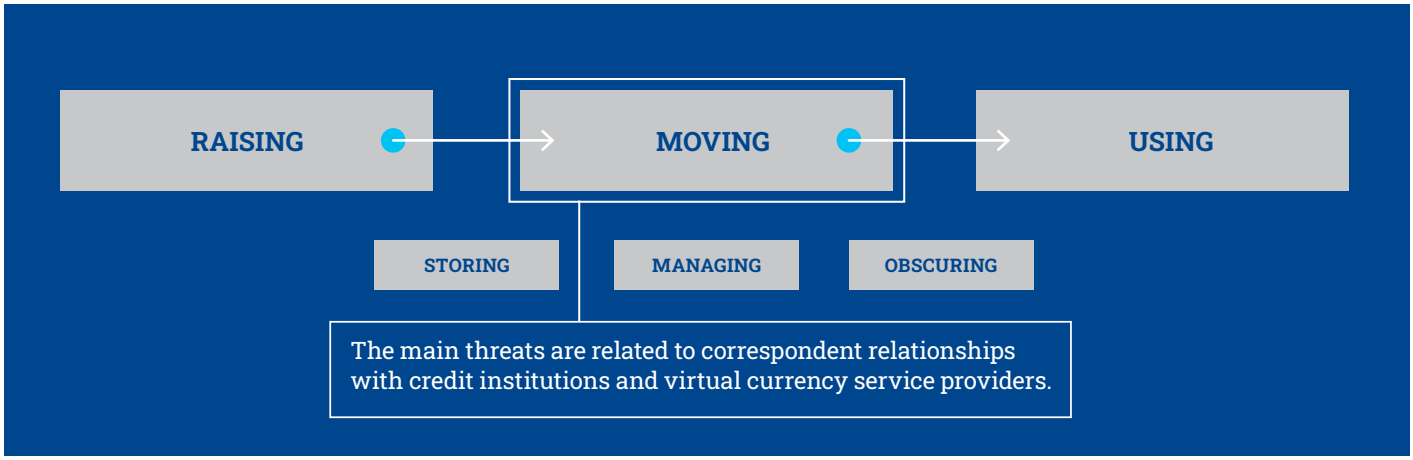




COUNTERING TERRORIST FINANCING

RISK PROFILE

- The terrorist financing **risk level in Estonia continues to be medium**.
- Estonia's economic environment is being used for the purpose of terrorist financing **in the moving stage**.



Cases involving terrorist financing are related to correspondent relationships to a significant degree. The FIU sees, for example, cases where a terrorist-linked or radicalised person living in a foreign country wants to make a transaction using a virtual currency service provider with an Estonian authorisation or a client of a credit institution. In addition, donations are observed in the correspondent relationships of credit institutions, primarily to foreign non-profit organisations that, among other things, also distribute messages of terrorist propaganda.

Ever more frequently, money is being sent for humanitarian purposes to unknown persons in conflict zones through crowdfunding campaigns. Such donations provide no room for control over the actual use of the funds. The senders of the funds are predominantly Estonian people, while the crowdfunding campaigns are foreign.

Market participants are increasingly detecting information indicating violent right-wing extremism, both through the information in transaction explanations and through increasingly skilful use of public sources.

In the previous yearbook, we described the trend of blurring extremist ideologies – the increasing intertwining of different ideological elements. This means that when analysing a suspicion of potential terrorist financing, it may be impossible for a market participant to identify a link to one specific ideology or movement. Now a new nuance has arisen – the importance lies in symbolism, not so much in ideology; it is the violence that provides excitement.

See the FIU's EFIUC 2025 conference for an overview of terrorist financing trends (in Estonian)

TERRORIST FINANCING IN NATIONAL RISK ASSESSMENT

One of the three reports of the national risk assessment addresses terrorist financing. The medium risk level of Estonia consists of the following:

- **below-average internal risk** – both the raising, moving and using of funds take place in Estonia
- **medium threat to other countries arising from Estonia** – increased sending of aid to conflict zones through crowdfunding campaigns; sending funds across borders to risk countries, including Central Asia
- **medium external threat** – mainly the Russian Federation, which in its own interests is looking for individuals for attacks and acts of sabotage
- **above-average transit risk** – mainly related to correspondent relationships, where transactions are intended to be made through a client holding an Estonian service provider's authorisation; persons with extremist ties travelling through Estonia and the risk of cash, debit cards and communication equipment being transported to conflict zones[3]

TERRORIST FINANCING REPORTS

138
terrorist financing reports were submitted

of which

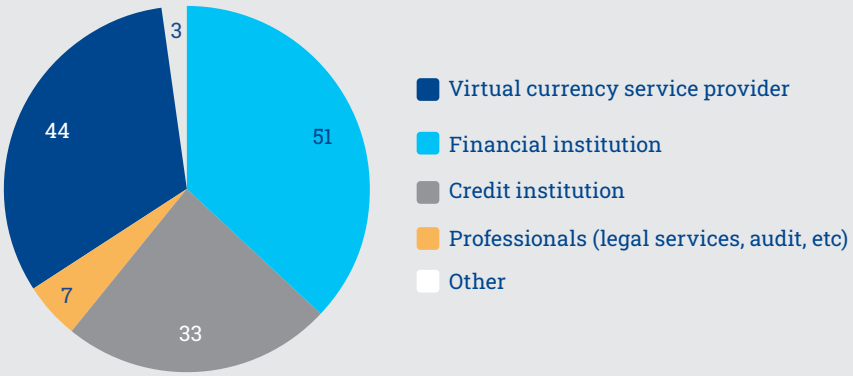
88%
due to higher terrorist financing risk and unusual element(s) potentially indicating terrorism (TFR-1)

12%
due to suspicion of terrorist financing (TFR-2)

In one case, the disposal of assets was restricted for 30 and 60 days in virtual currencies worth **1,319.47** euros.

The submission of terrorist financing reports has been stabilising in recent years, given the ratio of market participants. There are still sectors that file reports very rarely, such as providers of company services and currency exchange companies.

Number of terrorist financing reports by submitter



The median value of transactions reported was 150 euros in 2025 (approximately 300 euros the year before). Almost all reported transactions were cross-border transactions.

The following typologies are distinguished in the suspicion-based reports:

- according to blockchain analysis, the transaction took place in several intermediate steps;
- the transaction or action is carried out by a person who is potentially involved in violent extremism or has previously been convicted and served a sentence for terrorist financing;
- a donation has been made to a non-governmental organisation within the framework of a correspondent relationship with a credit institution, which shows support for the activities of a terrorist organisation.

Sectoral observations:

- **Financial institution reports** continued to report cross-border money transfers where the final identification of the counterparty is impossible. The main subject usually indicates a connection to fraud, but reports have also become more frequent where the main subject is a person living in a foreign country, in whose case a suspected connection to terrorism has been identified.
- **Credit institution reports** of 2025 showed more active reporting on the use of crowdfunding than before, where the parties have also been Estonian citizens. This is a continuation of the impact of the Israel–Hamas conflict. Reporting of donations to third countries also continued – sending funds to non-governmental organisations that, among other things, distribute Hamas propaganda videos.
- **Virtual currency service providers** continued to report transactions from crypto addresses and clusters categorised as terrorist-related, predominantly linked to Islamist extremism, but transactions by persons

who associate themselves with violent far-right ideology are also being reported. Information regarding online casinos and gambling has been added.

- There have been an increasing number of terrorist financing reports, which show identity theft or forgery of identity documents. This may indicate that monitoring is more sophisticated than before and that virtual currency service providers' remote identification programmes have become more effective. It may also indicate more active exploitation of clients of Estonian service providers.

5 YEARS

In Estonia, greater transparency and more effective dialogue have made a significant contribution to countering terrorist financing over the past five years. Cooperation with market participants has become more substantial. For the first time, the FIU invited a representative of a market participant for a two-month internship, which was part of the broader objective of strengthening risk recognition and enhancing information exchange. In developing the countering system, updating guidelines, consistent training of obliged entities, and creating information materials have played a central role. The list of high-risk countries is made publicly available on the website of the FIU. Market participants are expressing an increasingly clear understanding of the issue, and the reports submitted indicate the use of better monitoring tools and techniques. All of this has improved reporting of suspicions, helped identify an 18-member terrorist network in cooperation with market participants, and supported the country's successful completion of the UN assessment.

In 2025, 19 files related to potential terrorist financing were opened, which were based on reports from obliged entities as well as inquiries from foreign countries and the Estonian Internal Security Service. Most of the files opened based on the reports were related to virtual currencies and correspondent relationships between credit institutions.

THE RELATIONSHIP BETWEEN EXTREMISM AND TERRORISM

Terrorism is a method, a tool, a tactic. Extremism is an ideology, a belief system.

Terrorism is always politically motivated: the purpose of a terrorist crime is to instigate the overthrow of the existing government or undermine the social system by using violence or intimidating society. Terrorism is based on an extremist ideology, and every terrorist group is thus also extremist.

However, not every extremist group is officially a terrorist organisation. A person with extremist views may not necessarily support the use of violence. On the other hand, a person inspired by both a terrorist organisation and extremism can commit an act of terrorism.

From the perspective of prevention instruments, it makes a difference whether a movement is categorised as a terrorist organisation at the EU or UN level,[1] or not – the financial sanction framework applies to EU and UN lists. On the other hand, there are movements the objectives of which qualify as terrorist under the legislation of most jurisdictions, but which are not on the EU or UN lists. In this case, countries prohibit such activities of organisations according to their own lists.

Information indicating violent extremism may provide reasonable grounds to suspect terrorist financing – therefore, submitting a suspicion-based report to the FIU is extremely important.

BEST REPORT OF THE YEAR

The best report of 2025 comes this time from the field of countering terrorist financing. A virtual currency service provider filed a report related to the after-effects of the Israel–Hamas war.

THE STORY BEHIND THE REPORT

The client of a virtual currency service provider, licensed in Estonia, was a person residing abroad who made a direct payment in bitcoins to a crypto address belonging to a cluster from which Gaza Now forwarded essentially all the funds – worth 26 000 euros – to the exchange platforms.

Gaza Now features, among other things, body camera videos of Hamas fighters and has regularly organised appeals for raising funds to various crypto addresses. Although this does not apply in Europe, Gaza Now has been on the United States OFAC sanctions list since March 2024. The connection to a terrorist party can also be identified through public sources.

The service provider identified a suspicious transaction using its monitoring system and blockchain analysis tool, which was moved to manual inspection.

[1] At the time of compiling the yearbook, there were 13 natural persons and 22 organisations on the EU list, and 726 natural persons and 273 organisations at the UN level.

https://www.consilium.europa.eu/en/policies/sanctions-against-terrorism/,
https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list

The person attempted to use five bank cards issued in two different countries with the virtual currency service provider. Authentication failed for several cards for various reasons.

The person's main transaction pattern with the service provider was exchanging regular currency for virtual currencies.

No indications of suspicious activity regarding the person were found in public sources.

The service provider asked the person several times for additional information about the transaction and also investigated the origin of the funds, but the person declined to answer.

The market participant froze the person's account, which contained funds worth one thousand euros, and promptly filed a report with the FIU marked 'Urgent' to request further instructions.

STRENGTHS OF THE REPORT

- The report's description of the transaction had a logical structure and an easy-to-follow narrative that clearly answered the questions: **who, what, when, where, how, and why**. The following was provided: the main suspicion together with the transaction hash; more detailed information about the transaction and the terrorist party, the person's profile and account activity; account balance and account freezing information by the service provider; due diligence measures applied; the result of the analysis of public sources and a summary.
- The report clearly stated:
    - the account balance as a specific amount and a reference to the freezing of the account
    - results and inconsistencies in the application of due diligence measures
    - bank card information
    - result of collecting open-source intelligence (OSINT)
    - data on the person who made the transaction suspected of terrorist financing
- The following documents necessary for conducting analysis were attached to the report:
    - selfie and the person's documents
    - IP address logs together with timestamps
    - visual representation of the result of the blockchain analysis
    - account transactions (virtual currency, amount, transaction type, status, timestamp, and other such information) and card transactions
    - comprehensive analysis of the service provider

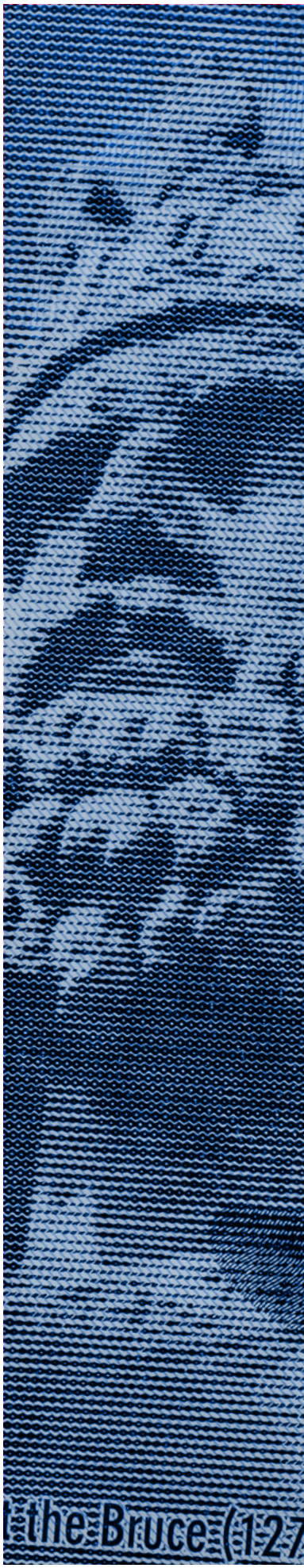
- The report was filed promptly while due diligence measures were still being applied.

WHAT MORE COULD THE SUBMITTER OF THE REPORT HAVE DONE?

- Clearly state whether the person has other wallets.
- Provide the device's so-called fingerprint with the stated IP addresses.
- Collect information from public sources in the person's native language.
- Check whether other clients of the service provider have logged in from the same IP addresses.
- Check whether there are other clients with the same phone number or address.

WHAT HAPPENED TO THE REPORT NEXT?

- The FIU commenced investigation on suspicions of terrorist financing, cooperating with the Estonian Internal Security Service. The FIU was previously aware that an investigation had been initiated abroad regarding the aforementioned terrorist party.
- Information was disseminated from Estonia to the person's country of residence and to the foreign country where the investigation into the terrorist party had been initiated.
- The FIU imposed a restriction on disposal of an account maintained by an Estonian virtual currency service provider for 30 days under a compliance notice based on subsection 1 of § 57 of the Money Laundering and Terrorist Financing Prevention Act and then a restriction on disposal for 60 days based on subsection 3 of § 57 of the Money Laundering and Terrorist Financing Prevention Act.
- The investigation is pending.





INTERNATIONAL FINANCIAL SANCTIONS

455

international sanctions reports were filed

248

reports received feedback from the FIU on the application of financial sanctions

RISK PROFILE

In 2025, sanctions evasion remained the primary focus. Although the number of cases analysed by the Financial Intelligence Unit has decreased compared to previous years, evasion schemes have become increasingly complex, often involving multiple countries within transaction chains. Sanctions violations due to ignorance are becoming less common – market participants and companies engaged in business with Russia are now better informed about the sanctions imposed on Russia.

Sanctions evasion schemes are becoming increasingly complex and international.

The phenomenon of jurisdiction shopping (where companies and persons relocate their business activities and bank accounts, at least in part, to another jurisdiction to circumvent EU sanctions), organised networks facilitating sanctions evasion and the key role of banks in countering sanctions evasion were discussed in more detail in the 2024 Yearbook of the FIU. These typologies have not disappeared. Sanctions violators continue to use complex transaction chains and multiple jurisdictions to conceal their true objectives and facilitate their activities. Compared to previous years, 2025 saw increased use of foreign virtual currency service providers and banks outside of Estonia to circumvent sanctions, primarily to move funds (through multiple intermediaries) from Russia to Estonia. Since the start of the full-scale Russian invasion of Ukraine, the awareness and capabilities of Estonian credit institutions have improved significantly. This has made it increasingly difficult for sanctions violators to transfer funds from Russia to Estonia, particularly from sanctioned banks.

The Financial Intelligence Unit has identified several cases where funds were moved through multiple parties and countries, with cash also being used in the final stages of the transactions. This indicates an attempt to obscure the original source of the funds and potential links to Russia and sanctioned entities. Such movement of funds often takes place outside the European Economic Area, making it difficult to trace, and the parties involved in the transaction chain cannot often be fully identified. To facilitate the transfer funds from Russian banks, payment intermediaries, banks and cryptocurrency exchange platforms in third countries (such as Turkey, Kazakhstan, Serbia) are often used, where sanctions are not applied to Russian sanctioned banks. Transaction chains often involve multiple parties to conceal the true origin of funds from EU-registered credit or financial institutions.

In 2025, several cases were identified where Estonian companies or persons held stakes in, or owned subsidiaries located either, in Russia or in third countries outside the EU. Through these entities, transactions are conducted with Russian counterparties, including certain sanctioned banks, with accounts mostly held by companies operating in Russia. Such schemes are used to avoid direct transactions between Estonia and Russia.

The Financial Intelligence Unit also received several reports of suspected money laundering, in which the predicate offence was a breach of trade sanctions. In addition to breaches of trade sanctions, several cases also indicated breaches of financial sanctions, where the end recipient of goods was a sanctioned person or funds were routed through sanctioned financial intermediaries.

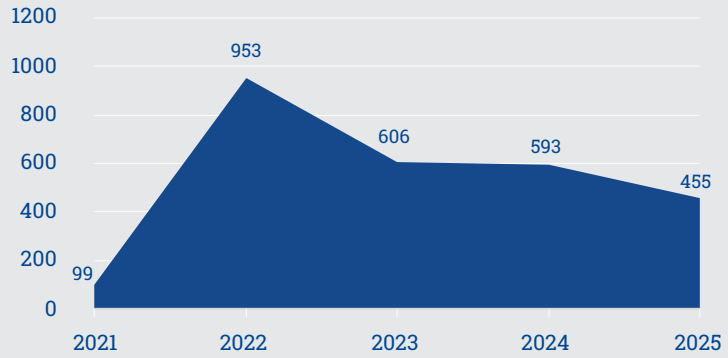
5 YEARS

Following the full-scale Russian invasion of Ukraine and the imposition of new, stringent sanctions by the EU, both public and private sector institutions were required to rapidly allocate significant additional resources. Over a five-year period, 20 sanctions packages were introduced, all of which had to be implemented immediately and in full. Knowledge of sanctions implementation increased significantly among both public sector institutions and market participants. Cooperation between institutions was further strengthened through handling of complex cases, such as fertiliser terminals located in Estonia and owned by entities subject to sanctions.

REPORTING

The number of reports related to international financial sanctions is on a downward trend. Compared to 2024, there were nearly one quarter fewer reports in 2025, and just over half as many as in 2022, when Russia launched its full-scale war in Ukraine. This is consistent with payment statistics, which show a decline over the years in both incoming and outgoing payments involving Russia and Belarus. Credit institutions have reviewed their risk appetite and customer portfolios. Moreover, there has been a decline in the activity of sanctioned entities associated with fertiliser terminals in Estonia, as well as in the numbers of related reports.

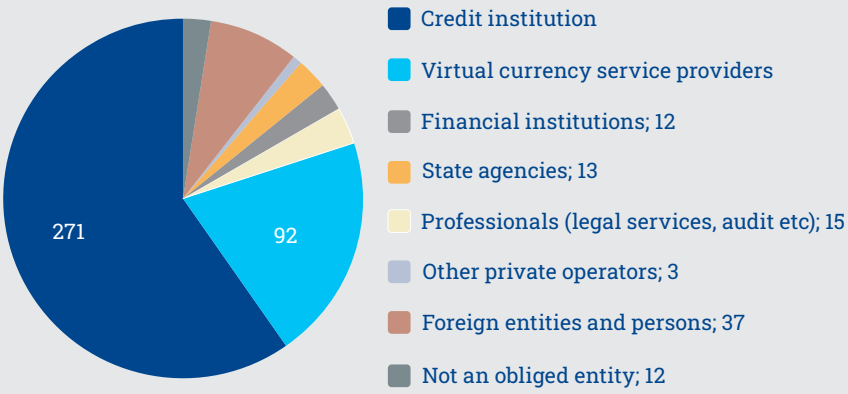
International financial sanctions reports (ISR)



Most reports were related to sanctions regimes imposed by the EU or the Government of the Republic of Estonia against Russia and Belarus. In most cases (80%), market participants correctly assessed the need to apply financial sanctions or applied them lawfully. In cases where, according to the FIU´s assessment, sanctions did not need to be applied, or where a market participant had applied measures unlawfully, guidance for further action was provided. These cases mainly involved situations where the person could not be identified and additional information from the FIU helped to rule out a sanctioned entity. Of the restrictive measures applied, the freezing of funds was the most common, while in one third of cases transactions were refused, meaning that funds were not made available to sanctioned entities.

Virtual currency service providers have had to apply an increasing number of sanctions-related restrictions.

Filling of international sanctions reports



In 2025, the number of reports received from virtual currency service providers that required feedback on the application of financial or sectoral sanctions increased significantly. The main reason for the increase in such virtual currency-related reports was the inclusion of Garantex – a cryptocurrency platform that held an authorisation in Estonia until 24 February 2022 – on the EU sanctions list on 24 February 2025. Previously, OFAC sanctions applicable to Garantex were not binding on Estonian market participants. However, once Garantex was included on the EU sanctions list, market participants engaging with the platform became subject to an obligation to apply sanctions. In the analysed cases, the exposure of authorised Estonian virtual currency service providers to Garantex was indirect in most instances and primarily related to customers who conducted transactions linked to Garantex.

The increase in the number of reports was also driven by the more frequent application of sectoral sanctions in cases where virtual currency service providers suspected that a customer might be a citizen of Russia or Belarus

and no longer reside in the European Economic Area or Switzerland. While the ability of credit institutions to identify suspected breaches of financial sanctions has improved over time, concerns remain regarding the underreporting of transactions by Estonian virtual currency service providers and their limited capacity to detect transactions that violate the EU sanctions.



NEW RESTRICTIONS AND REGULATIONS

EUROPEAN UNION SANCTIONS PACKAGES IN 2025

In 2025, the EU adopted four packages of sanctions against Russia and Belarus, adding 331 new names (133 natural persons and 198 entities) to the sanctions lists. The lists included, inter alia, companies supporting the Russian military industry and their international partners; individuals involved in the deportation of Ukrainian children; disseminators of disinformation; Russian military-industrial companies and their leaders and suppliers; those aiding in the circumvention of sanctions; companies linked to the shadow fleet; and high-ranking North Korean military officials.

The new sectoral financial sanctions primarily focus on restricting the movement of funds between Russia and other countries. The most significant measures include:

1. a full transaction ban on Russian banks with access to EU financial messaging services (extended to a further 22 banks);
2. a prohibition on EU operators engaging with the Russian Mir and SBP payment systems;
3. an expanded ban on transactions with banks in Russia and third countries, including in cases of violations of the oil price cap or incidents involving the shadow fleet;
4. a prohibition on issuing new payment instruments to citizens of Russia and Belarus and on providing crypto-asset services to them.

In addition, the provision of services to the governments of Russia and Belarus was prohibited without prior authorisation. In the case of financial services, applications for such authorisation must be submitted to the FIU.

In 2025, the EU removed Viatcheslav Moshe Kantor from its sanctions list following a request from one Member State. Estonia subsequently included him in its national sanctions list, which required existing authorisations to be reissued, but the restrictive measures remained in force.

INTRODUCTION OF A REGULAR REPORTING OBLIGATION ON FROZEN ASSETS FOR PERSONS SUBJECT TO SPECIAL OBLIGATIONS

On 1 January 2025, a requirement for persons subject to special obligations to submit reports to the FIU entered into force. These reports are primarily used to verify compliance with financial sanctions obligation.

REPORTING ON FROZEN ASSETS[2]

Credit institutions and virtual currency service providers must submit reports four times a year for each completed quarter. Two reports must be submitted:

- a report on the movement of funds in accounts frozen as a result of the application of international financial sanctions, i.e. funds credited to frozen accounts of sanctioned entities during the reporting period, and payments made from such accounts on the basis of authorisations;
- a report on funds frozen in their possession as a result of the application of international financial sanctions that are not reflected in the report submitted pursuant to subsection 1, i.e. situations where transactions are received by or directed to a sanctioned entity;

Other persons with special obligations must submit reports once a year on the frozen funds and economic resources in their possession that result from the application of international financial sanctions.

NEW FINANCIAL SANCTIONS GUIDELINES OF THE FINANCIAL INTELLIGENCE UNIT

On 30 May, an updated guideline and a new guideline of the FIU entered into force.

The FIU's updated guideline on the application of financial sanctions[15] is addressed to all persons applying financial sanctions in Estonia, including those who are not persons subject to special obligations. The guideline provides an overview of sanctioning authorities, types of sanctions, financial sanctions and requirements for their application , the scope of the obligation to freeze assets and the prohibition on making them available, the application of the ownership and control criterion, the obligation to submit notifications and reports to the

[2] Established by Regulation of the Minister of Finance of 28 March 2025 'More detailed composition and provider of and procedure for submission of data in the reports submitted to the Financial Intelligence Unit by persons with special obligations', RT I, 02.04.2025, 7. https://www.riigiteataja.ee/akt/102042025007

FIU, and exemptions to financial sanctions. The annexes include examples of common methods of breaching and circumventing financial sanctions, as well as potential risk indicators of proliferation financing. The guideline also introduces a new recommended application form for financial sanctions authorisation.

The newly issued guideline is also intended for persons subject to special obligations providing services in Estonia and subject to supervision by the FIU[16]. The guideline sets out more detailed requirements for sanctions due diligence measures and for the development of organisational solution.

The new application form for financial sanction authorisation must be used.

IMPLEMENTATION OF FINANCIAL SANCTIONS AND ENSURING THEIR LAWFUL APPLICATION

UNDER FINANCIAL SANCTIONS:

45 authorisations for **derogations** were granted

as of 31 December 2025, frozen funds in Estonia amounted to nearly **46** million euros

funds exceeding **220,000** euros were not made available

a deposit restriction totalling **437,000** euros was applied

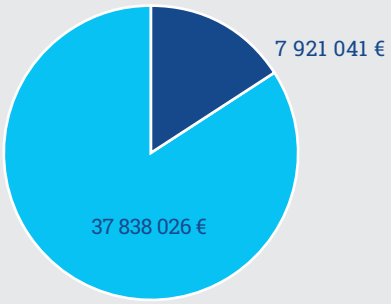
13 disclosures relating to sanctions were made to Estonian investigative authorities, and 4 to foreign investigative authoritiese[3]

71 requests for clarification regarding financial sanctions were answered

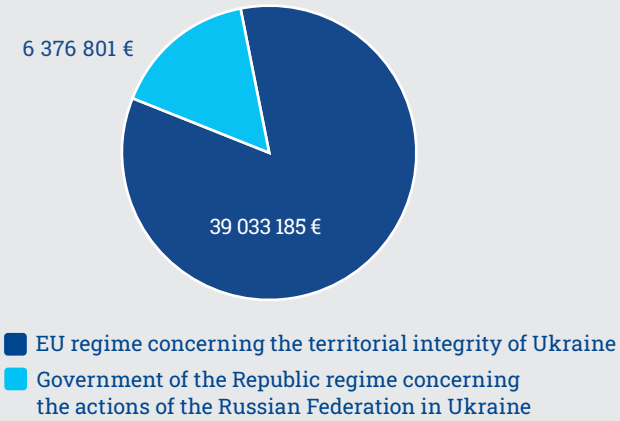
[3] In addition to financial sanctions, these also included disclosures concerning violations of import and export restrictions, of which information had been received by the Financial Intelligence Unit.

As at the end of 2025, funds totalling approximately EUR 46 million (EUR 42 million at the end of 2024) were frozen in Estonia. This amount is comparable to the level of frozen funds a year earlier. In addition, Estonia also holds frozen economic resources that are directly or indirectly owned by persons on the sanctions list and held by sanctioned entities.

Breakdown of frozen funds



Frozen funds by sanctions regime



More funds have been released under derogations than have been frozen. Based on a derogation authorisation and an existing agreement, payments may be made to accounts of the sanctioned entities held in Estonian credit institutions, provided that the funds remain frozen. At the same time, the FIU has, on the basis of previously concluded agreement, permitted payments that are necessary to ensure the safety and minimum functioning of companies related sanctioned entities – for example, for the payment of utility bills. These payments, in turn, reduce the overall amount of frozen funds.

The majority of derogations were related to the Muuga and Sillamäe chemical terminals, many of which were in turn linked to the sanctions imposed by the Government of the Republic of Estonia against Kantor.

In 2025, the FIU made 13 disclosures to investigative authorities concerning suspected breaches of financial sanctions, compared to 34 in the previous year. The decrease is partly attributable to a transfer of competence for investigating offences related to breaches of trade sanctions to the Estonian Tax and Customs Board, to which obliged entities began submitting such reports directly.

The steady volume of requests for clarification indicates a continued need for interpretative guidance in connection with new regulations and amendments to existing ones.

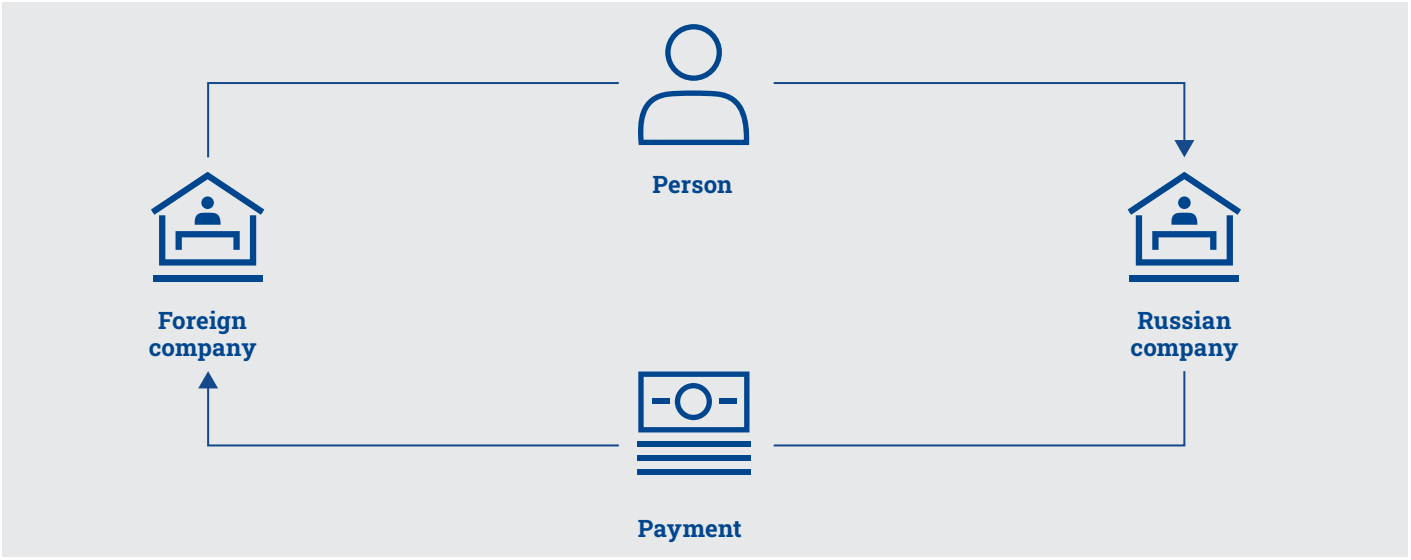
A financial sanction is not violated merely by making a payment to a person included on the sanctions list or by failing to freeze the funds held in that person's bank account. The making available of economic resources to a listed person is likewise prohibited. The volume of payments rejected by persons subject to special obligations who reported to the FIU has increased severalfold compared to earlier periods; however, this is increase does not reflect a change in trend but is attributable to a single exceptionally large payment. The EU interprets the concept of 'economic resources' broadly, and it does not cover only tangible assets.

WORKING FOR OR PROVIDING SERVICES TO A SANCTIONED ENTITY

During 2025, the FIU identified several cases in which an Estonian citizen or a person residing in Estonia worked for a listed person, or for a company owned or controlled by such a person, or provided services to that person or company. The funds received for the work performed or services provided were credited to the individual's bank account via a foreign company. The purpose was to conceal links to the sanctioned entity and to circumvent restrictions imposed by Estonian credit institutions on payments related to Russia.

In these cases, a violation of financial sanctions by an Estonian citizen or a resident lay in making economic resources available to a sanctioned entity through employment or the provision of services. According to the European Commission Opinion of 19 June 2020[4], the objective of the prohibition on making economic resources available to listed persons aims to prevent such persons from using those resources to obtain funds, goods or services. The European Commission considers that performing work or providing services to an entity owned or controlled by a listed person may be regarded as indirectly making economic resources available to that person, if such activity enables the latter to obtain funds, goods or services.

Each case is assessed individually; however, if a listed person can use the proceeds of a specific job or service to obtain funds, goods or services, those proceeds are considered to have been made available to them and, consequently, such activity constitutes a breach of financial sanctions.



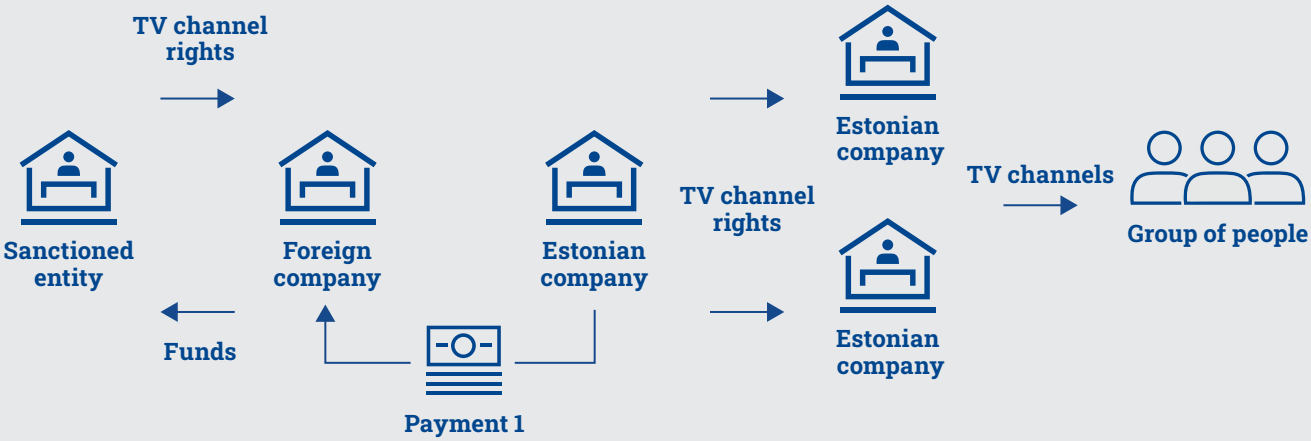
TRANSMISSION OF TELEVISION CHANNELS

In 2025, there were cases in which an Estonian company acted as an intermediary for the broadcasting rights of television channels owned by a sanctioned entity. The Estonian company had purchased these rights from a foreign company rather than directly from the sanctioned entity.

First, it must be assessed whether such activities result in a listed earning income, i.e. through which intermediaries and to whom the fees for broadcasting or transmitting television channels ultimately flow.

Secondly, it is important to note that a breach of financial sanctions may already occur through the transmission or broadcasting of television channels owned by a listed person. The European Commission takes the view that the distribution of television channel content constitutes an economic resource, as it increases the visibility of such channels (thereby potentially generating new customers), and the content may be used advertise products and services, thereby generating revenue for its owner[5, lk 316].

The FIU contacted companies distributing these television channels to draw their attention to the fact that, even where no payment is made to a sanctioned entity, the distribution of such channels may constitute a breach of the sanction's regulation.



Watch the FIU conference presentation on Europol's PPP cooperation in sanctions enforcement

PROLIFERATION FINANCING

FATF REPORT ON SANCTIONS EVASION

In June 2025, the Financial Action Task Force (FATF) published the report 'Complex Proliferation Financing and Sanctions Evasion Schemes'[6]. The report aims to provide an up-to-date practical overview of proliferation financing with particular focus on how relevant networks attempt to circumvent financial sanctions and other restrictions.

The report focuses on four key typologies of proliferation financing and sanctions evasion.

It confirms that the risk of sanctions evasion related to proliferation financing remains significant and emphasises that effective results can only be achieved through consistent risk management, effective cooperation and continuously evolving countermeasures. The report integrates strategic risk analysis, practical typologies and implementation experience into a coherent framework that can be used to refine national risk assessments, set supervisory priorities and develop private sector control measures.

REINSTATEMENT OF UNITED NATIONS SECURITY COUNCIL AND EU SANCTIONS ON IRAN

As Iran failed to substantially comply with its obligations under the Joint Comprehensive Plan of Action (JCPO[4]), the UNSC did not support the extension of the suspension of sanctions, and UN sanctions on Iran were reinstated as of 27 September 2025. The EU restrictive measures against Iran also came back into force on 30 September 2025. The reinstated measures include both those adopted by the UNSC in 2006 and the EU´s autonomous measures.

The reinstated financial sanctions include the freezing of assets of listed persons and entities, as well as prohibitions on investment and financial services. The assets of the Central Bank of Iran and major commercial banks were again frozen. Additional economic restrictions were also imposed, including restrictions on trade and transport, import bans on Iranian crude oil, gas and petrochemical products, and travel bans on listed persons.

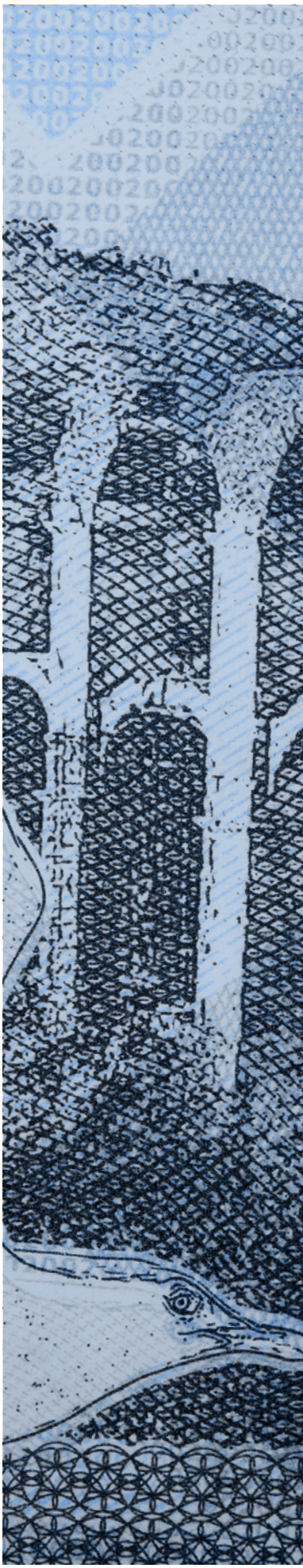
COUNTERING PROLIFERATION FINANCING IN THE NATIONAL RISK ASSESSMENT

In addition to reports on the prevention of money laundering and terrorist financing, a national risk assessment on proliferation financing[7] was prepared and adopted, based on data analysis covering the period 2020–2024.

According to the assessment, Estonia's exposure to proliferation financing is currently low; however, the level of vulnerability is increased due to the geographical proximity of, and historical trade ties with Russia, which is involved in proliferation financing. Estonian territory may be used for the transit of goods to Russia, and from there, to North Korea or Iran.

The report assesses that in Estonia:

- the threat level of violations or non-application of targeted financial sanctions is low, with risks primarily arising from market participants who may be exploited to commit such violations;
- the threat level of evasion of targeted financial sanctions is medium, driven in part by Russia's close cooperation with Iran and North Korea;
- the level of vulnerability to violations or non-application of targeted financial sanctions is low, as Estonia's legal framework is sufficient for the effective prevention of proliferation financing;



[4] The Joint Comprehensive Plan of Action is a comprehensive plan of action regarding the nuclear program of Iran, which established a timeline and procedures for lifting nuclear-related sanctions imposed on Iran.

- the level of vulnerability to the evasion of targeted financial sanctions is low; as of the end of 2024, effective mitigation measures have been implemented for most identified vulnerabilities. For example, vulnerability in the virtual currency service provider sector has decreased due to a reduction in the number of market participants and the introduction of additional supervisory measures.



AUTHORISATIONS AND SUPERVISION

AUTHORISATIONS

As of 31 December 2025, there were

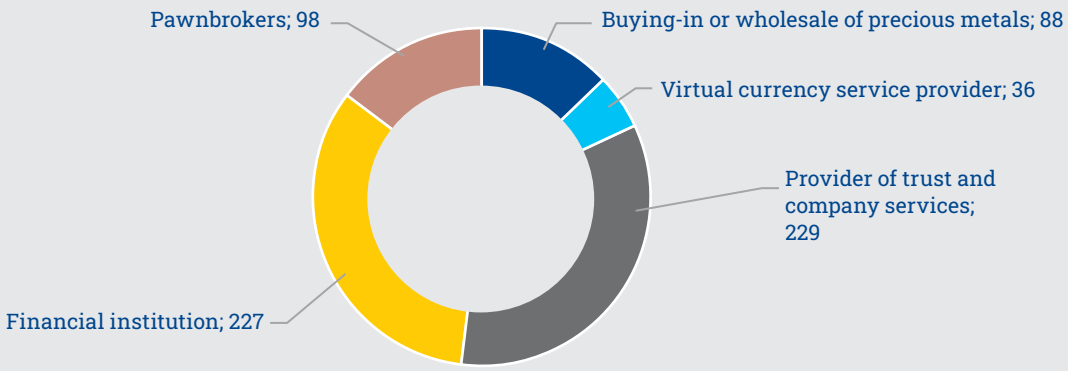
678 valid authorisations issued by the Financial Intelligence Unit

19 new authorisations were issued

76 authorisations expired

164 procedures for obtaining or amending an authorisation were completed

Authorisations issued by the FIU as of 31 December 2025



5 YEARS

The most significant change has occurred in the streamlining of authorisations for virtual currency service providers. The sector was primarily affected by legislative amendments aimed at mitigating money laundering risks that had emerged in the country, as well as by the resulting supervisory activities of the Financial Intelligence Unit. From 846 authorisations at the beginning of 2021, only 36 remained by the end of 2025. We described the journey of streamlining the sector in our 2023 Yearbook.

Of the 19 new authorisations issued:

- 11 were granted to financial institutions, including 8 to small fund managers – more than previously;
- 7 to providers of trust and company services;
- 1 to a pawnbroker.

Most applications for new authorisations were submitted by financial institutions.

The main reasons why companies were not granted authorisations were deficiencies in their anti-money laundering and countering the financing of terrorism (AML/CFT) documentation, which applicants failed to remedy despite repeated remarks from the Financial Intelligence Unit. In two cases, the FIU found that the business reputation of persons associated with the applicant was not adequate.

The number of judicial proceedings related to authorisation procedures has decreased year on year. In 2025, three new disputes were initiated concerning authorisation proceedings: two decisions to revoke authorisations and one decision refusing to amend an authorisation were challenged.

Holding an authorisation entails responsibility.

A total of 76 authorisations expired, including:

- 55 cases where companies voluntarily surrendered their authorisations, either during supervisory proceedings or due to other circumstances. In the chapter on supervision, we see that authorisation applications are sometimes submitted without sufficient consideration of the responsibilities involved;
- 4 cases where the Financial Intelligence Unit revoked the authorisation, mainly due to failure to submit annual reports and in one case due to non-compliance with a compliance notice;
- 8 authorisations that ceased to be valid as a result of company mergers, where the legal successor already held an authorisation or did not apply for one;
- 9 authorisations that expired following the deletion of the company from the commercial register.

PLEASE NOTE

- Companies are required to ensure that both their contact information and the details of their compliance officers are accurate in the relevant registers.
- It is important to keep internal company documents up to date on an ongoing basis in order to keep pace with the evolving risk environment.
- A small customer portfolio or a local market does not preclude exposure to money laundering or terrorist financing. This is a common misconception among undertakings with lower risk appetites, typically smaller companies, which often view the establishment of such systems as an unnecessary expense. This makes them easy targets for money laundering schemes.

Watch the Financial Intelligence Unit's EFIUC 2025 conference presentation on corporate compliance culture (in Estonian)

SUPERVISION

A total of **18** supervisory proceedings were carried out, including

7 on-site inspections

11 off-site inspections

Obliged entities are the first line of defence against money laundering and terrorist financing, and they are required to know their customers when providing services. They act as gatekeepers, protecting our society from criminals seeking to exploit the Estonian financial and non-financial sectors for their own purposes. Supervision in AML/CFT involves verifying whether obliged entities have the required procedures and internal systems in place to fulfil their role in preventing money laundering. Supervisory findings help obliged entities to improve their systems.

RISK-BASED SUPERVISION

Supervisory activities carried out in 2025 revealed significant shortcomings in the awareness of obliged entities. Documentation that has not been updated for years indicates that risks have not been reassessed – neither following the publication of the national risk assessments in May 2021 and October 2025, nor in response to the sanctions introduced in connection with Russia's full-scale invasion of Ukraine in 2022. More information on shortcomings in higher-risk sectors can be found in the following subsections.

In more than half of supervisory cases, the following were identified:

- deficiencies in the risk assessment, risk appetite definition, rules of procedure and/or internal control rules within the meaning of both the Money Laundering and Terrorist Financing Prevention Act and the International Sanctions Act;
- deficiencies in the application of due diligence measures under the Money Laundering and Terrorist Financing Prevention Act.

AWARENESS-RAISING

The Financial Intelligence Unit prepares guidelines and advisories, organises information events and participates in co-operation meetings with sector representatives. The aim is to raise the awareness of obliged entities of both the deficiencies identified during supervision and the trends related to the risks of international money laundering and terrorist financing.

5 YEARS

The Financial Intelligence Unit has taken a direction towards being more market-facing than before. Dialogue gives market participants better opportunities to understand the intent of the legislator and helps supervision to better understand the specific characteristics of different sectors. For example, we informed the gambling sector six months in advance that we would begin conducting on-site inspections.

In 2025, the following were targeted at subjects of supervision:

- 4 advisories issued to gambling operators, virtual currency service providers and, on two occasions, to providers of company services. The advisories provided obliged entities with sector-specific guidelines on mitigating money laundering and terrorist financing risks.
- 25 information events out of 35 events organised by the Financial Intelligence Unit, which were aimed directly or partly at obliged entities, with the objective of providing recommendations for improving their systems. As part of the EFIUC 2025 conference, the FIU organised a simulation exercise involving international consultants, to which a total of 42 representatives from company service providers, virtual currency service providers, notaries and banks were invited.
- 5 co-operation meetings with representatives of different sectors, where the perspectives of market participants and sector-specific characteristics were discussed, and the Financial Intelligence Unit provided obliged entities with guidance on improving their AML/CFT systems.

In addition, ten supervision-related meetings were held with Estonian authorities and three with foreign counterparts.

In connection with the update of the guidelines on the application of due diligence measures for obligated entities, the FIU sought sector-specific proposals from several umbrella organisations and market participants. The guidelines will be published in the second half of 2026.

Watch the video on the application of due diligence measures (in Estonian)



FINANCIAL INSTITUTIONS

As of 31 December 2025, there were **227** valid financial institution authorisations

5 supervision operations were carried out, including

1 on-site inspection

4 off-site inspections

According to the national risk assessment (2025), the following are above average:

- the level of money laundering risk and vulnerability of financial institutions;
- the level of money laundering risk of payment institutions and e-money institutions;
- the level of vulnerability and residual risk of management companies.

Financial institutions will require increased supervisory attention in the coming years. The main deficiencies identified during supervision in relation to compliance with the documentation requirements of both the Money Laundering and Terrorist Financing Prevention Act and the International Sanctions Act were as follows:

- Risk assessment – not up to date; either absent at the level of the company as a whole or not distinguished from the principles for determining the customer risk profile; risks associated with the provision of specific services are not identified (eg what risks a lender must consider, assess and mitigate); identified risks are not assessed or analysed, meaning that the nature of the risks, their level and mitigation measures are not understood; the risk assessment does not cover risks related to financial sanctions, including proliferation financing.

- Risk appetite – too vague and not up to date; quantitative indicators are entirely absent from the risk appetite or do not correspond to the actual activities of the company (eg how many high-risk customers the company is prepared to serve); there is no definition of risk appetite from the perspective of financial sanctions, including proliferation financing.
- Rules of procedure – not up to date and do not correspond to the actual activities of the company or legal requirements; too vague and do not contain detailed instructions for the application of due diligence measures; do not contain instructions related to financial sanctions, including proliferation financing.
- Internal control rules – either entirely absent or very vague; there are no procedures for the functioning of the internal control system or detailed instructions.

Off-site inspections conducted by the Financial Intelligence Unit of lenders and small fund managers also revealed that several companies have not updated their rules of procedure, risk assessments and/or risk appetite documents since obtaining their authorisation or, at the very least, over the past five years.

To operate as a lender, an authorisation must be obtained from:

- the Financial Supervision Authority if the company is not a credit institution and intends to grant loans to consumers, ie natural persons, provided that the granting of such loans is not related to the independent economic or professional activities of these persons;
- the Financial Intelligence Unit if loans are granted to non-consumers, ie primarily legal persons and self-employed persons

If a company intends to grant loans to both consumers and legal persons, only an authorisation from the Financial Supervision Authority is required – a separate authorisation from the Financial Intelligence Unit is not required.

The granting of authorisations to lenders is governed by the Law of Obligations Act, the Creditors and Credit Intermediaries Act, the Credit Institutions Act and the Money Laundering and Terrorist Financing Prevention Act.

The Financial Intelligence Unit carries out AML/CFT supervision and has found that the business models and investment strategies of small fund managers vary significantly, which increases the importance of risk assessment. For example, investments are made in wine, as well as in start-ups and early-stage companies. Early identification, assessment and mitigation of risks require an appropriate organisational structure, awareness at all levels, management support and relevant training.

ACTIVITIES OF UNAUTHORISED LENDERS

An analysis based on public data revealed that two lenders holding an authorisation from the Financial Intelligence Unit were granting loans to natural persons. This raised suspicions that the companies were operating without a valid credit provider authorisation from the Financial Supervision Authority. Under an authorisation issued by the Financial Intelligence Unit, lending is permitted only to legal persons. The companies were contacted, asked to provide explanations and informed of the circumstances under which lenders must apply for an authorisation from the Financial Supervision Authority. Suspicions of possible unauthorised activity were forwarded as a criminal report to the investigative authority for further investigation.

SUSPICIONS REGARDING THE ACTIVITIES OF A LENDER IDENTIFIED DURING SUPERVISION

A lender holding an authorisation from the Financial Intelligence Unit and its customer base were characterised by:

- the lender's shares in and/or an account held with a credit institution in Montenegro and/or Ukraine, where also 90% of the accounts of the lender's legal person customers were held;
- the Estonian lender granted 90% of loans to legal person customers from accounts held with its affiliated credit institutions in Montenegro and Ukraine;
- 63% of customers originated from countries with a high risk of corruption (Montenegro and Ukraine);
- customers were found through personal connections, with no marketing activities carried out to acquire customers;
- several customers have been the subject of negative media coverage in connection with corruption, arms trafficking and organised crime.

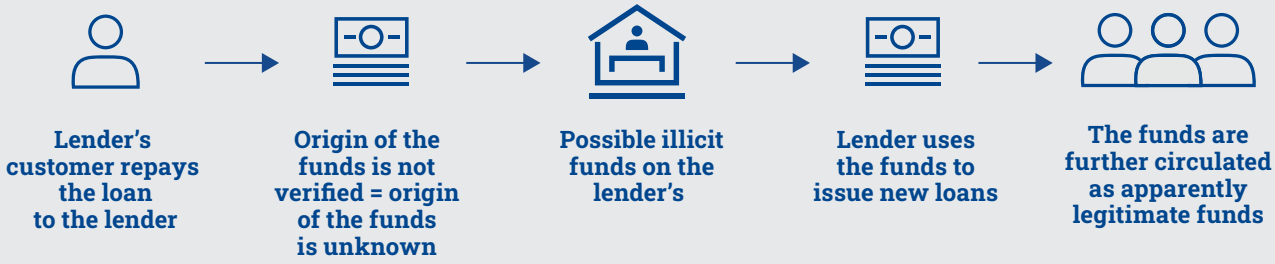
Supervision revealed that the lender failed to:

- verify the identity of the representatives of the customer;
- identify the beneficial owners of the customers;
- verify the authenticity of identity documents (possible indications of document forgery);
- gather information on the origin of property used in the transactions as well as on the source and origin of the customer's wealth.

The supervisory proceedings revealed circumstances that indicated possible money laundering in the activities of the customers. The lender did not verify the source and origin of loan repayments, although loans were granted to customers on a short-term basis, ranging from one week to one month, in amounts from 800,000 to 2 million euros, primarily for working capital financing. It is noteworthy that loans with the same term and amount were repeatedly granted to the same customers. In addition, during supervision it was established that one private person transferred amounts reaching millions to the lender's bank account and the lender then transferred the same amounts as a loan on the same day or a few days later to a company associated with that same private person.

The funds, which were not verified, may have been of illicit origin and the subsequent use of the funds for the issuance of new loans may indicate the apparent legitimisation of funds.

Lender as a money-laundering machine



As a result of supervision, the lender applied additional due diligence measures to its customers and will be better able to fulfil its role in preventing money laundering in the future – paying greater attention to customer relationships, verifying the origin of property when loans are repaid and reporting any lingering suspicions.

PROVIDERS OF COMPANY SERVICES

As of 31 December 2025, there were **229** valid authorisations for the provision of company services

10 supervision operations were carried out, including

3 on-site inspections

7 off-site inspections

> According to the national risk assessment (2025), the level of money laundering risk and vulnerability among providers of company services is above average.

On the one hand, overall awareness within the sector is on the rise and the supervisory authority maintains close communication with the majority of market participants. On the other hand, the results of 2025 supervisory proceedings and off-site inspections carried out in April confirm a continuing trend: a numerically small but, in terms of market share, significant portion of trust and company service providers do not sufficiently recognise their role in mitigating the risks of money laundering and terrorist financing. Supervisory proceedings revealed that, in certain parts of the sector, there is still a lack of understanding regarding the role of the service provider as a first line of defence – or gatekeeper – who is the first to encounter suspicious activity and is capable of identifying schemes before they reach the broader financial system. Some market participants treat anti-money laundering measures merely as an inconvenient administrative burden, without considering their true purpose and value.

To foster a culture of anti-money laundering and to build understanding and trust, the FIU maintains ongoing communication with representatives of obliged entities outside supervisory proceedings. For example, we met with a representative of a trust and company service provider, explained the activities of the Financial Intelligence Unit and the reasons for why we use such measures, as well as how they help mitigate risks. As a result of the meeting, the obliged entity gained a better understanding of the activities of the FIU and the FIU gained a better understanding of the company. Such a meeting laid a solid foundation for future communication in supervisory proceedings.

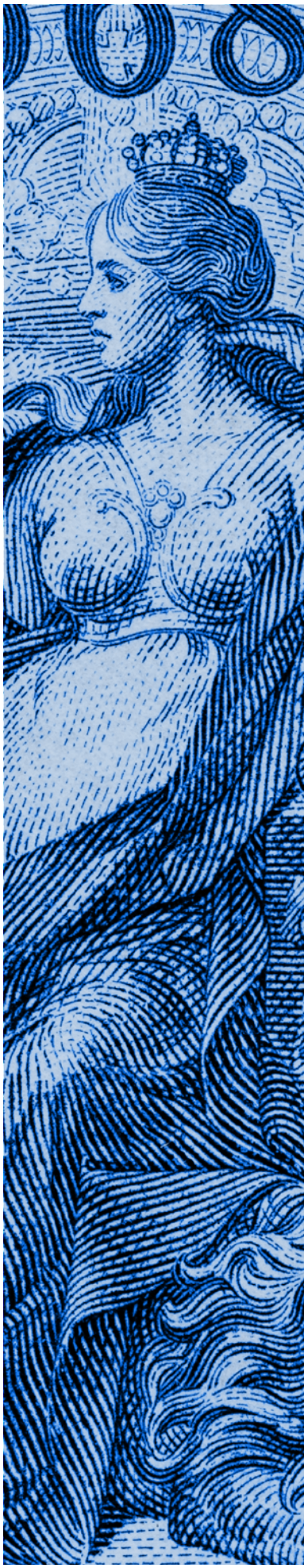
During supervisory proceedings, we found that many companies have relevant documents and procedures in place only in appearance, ie they have been prepared for presentation to the supervisory authority rather than for use in their own operations. In addition, the following systemic deficiencies were identified:

- Lack of documentation – 15.5% of respondents did not have in place the rules of procedure required under the International Sanctions Act and 21% lacked an adequate risk management system.
- Poor application of due diligence measures: as of the end of 2024, more than half of service providers had not applied enhanced due diligence measures to any customers, even when serving customers from high-risk countries such as Russia, Belarus or Iran.
- Low reporting activity: only 4% of the sector submits suspicious transaction reports. In 2024, 86.7% of respondents did not identify any suspicions, despite known incidents or risks associated with the provision of services and the nature of customers and services, suggesting that threats are either not being identified or are being deliberately overlooked.

During inspections, five service providers surrendered their authorisations, apparently to avoid receiving or complying with compliance notices or further proceedings. A possible scheme to circumvent supervision also emerged: as soon as the state begins to show interest, the company surrenders its authorisation and continues its activities under another authorised company that has not yet come under supervisory scrutiny.

A total of two advisories were issued to providers of trust and company services during the year. One advisory drew the attention of the entire sector to the deficiencies identified in risk management. The second advisory was issued to service providers who were required to update their compliance officers.

Despite the common understanding that has been reached, there remains a continued need in the sector for consistent efforts to increase knowledge and harmonise the quality of due diligence measures. Money laundering and terrorist financing schemes are constantly evolving, requiring service providers to keep up with increasingly complex typologies. The FIU will continue to organise sector-wide meetings to explain statutory requirements and provide practical guidance on the assessment and mitigation of risks.



IDENTIFIED SCHEME TO CIRCUMVENT STATE SUPERVISION

- The owners of C OÜ and A OÜ, companies holding an authorisation from the Financial Intelligence Unit as trust and company service providers, are AB and CD.
- C OÜ failed to comply with the compliance notice issued by the FIU and surrendered its authorisation immediately after the initiation of supervision proceedings.
- The turnover of A OÜ subsequently increased significantly.
- The Financial Intelligence Unit had no overview of the activities or customers of A OÜ, as the company had no economic activity at the time of completing the off-site inspection questionnaire in 2022 and the questionnaire was submitted with zero values.
- The Financial Intelligence Unit subsequently initiated supervision proceedings in respect of A OÜ.
- A OÜ failed to comply with the compliance notice and surrendered its authorisation immediately after the initiation of supervision proceedings.
- Although A OÜ was active in 2024, the company did not complete the 2025 off-site inspection questionnaire due to the surrender of its authorisation.
- The Financial Intelligence Unit terminated the supervision proceedings.
- In the case of A OÜ, there were grounds to suspect that the company had not adequately fulfilled its reporting obligation, as it had not submitted any reports.
- C OÜ had previously provided a sub-service to company D, which holds an authorisation in the same field in Lithuania. There are indications that this activity is now carried out by A OÜ and that a Lithuanian licence is being used for the provision of services.

The identified scheme raises questions about the transparency of the activities of the companies and their owners, as well as their underlying intentions. Beyond the question of how effectively money laundering is actually being prevented, such practices risk ultimately undermining the credibility of the entire Estonian trust and company service provider sector.

GAMBLING OPERATORS

As of 31 December 2025, there were **58** valid authorisations for the organisation of gambling

Of these, **45** were active operating permits, including

40 for the provision of remote gambling

2 for both casino and online gambling

2 for land-based casinos

1 on vessels and online

1 supervisory procedure was carried out

i

According to the national risk assessment (2025), the level of money laundering risk and vulnerability among gambling operators is above average and the residual risk level is high.

Growth in the gambling market is evident across Europe[8], particularly among remote gambling service providers. In Estonia as well, the number of service providers holding a gambling operator's authorisation has more than doubled over the past four years.

KEY AMENDMENTS TO THE GAMBLING ACT

- As a result of amendments to the Gambling Act, as of 1 January 2026, authorisations for organising gambling issued by the Estonian Tax and Customs Board must receive the approval of the Financial Intelligence Unit.
- Companies applying for an authorisation must submit the following together with their application, and companies holding an authorisation must, by 1 January 2027, ensure that the following are in place:
  - AML/CFT rules of procedure and internal control rules;
  - appointed compliance officer of the Financial Intelligence Unit;
  - additional documents concerning persons related to the applicant.
- The Financial Intelligence Unit assesses the submitted documentation for compliance with legal requirements and the suitability of the compliance officer for their role. If the documentation is compliant and the compliance officer is deemed suitable, the application is approved.

In supervision, the FIU focused primarily on critical risk indicators in this sector.

- First, the origin of customer's property and any unclear sources of funding are monitored. For example, the FIU monitors situations to determine whether companies are able to identify cash deposits made immediately before gambling or transfers from unknown third parties and foreign payment institutions that have no logical link to the customer's profile.
- Second, the focus is on gambling patterns and the use of straw persons. In this sector, a common typology is that persons with a criminal background use straw persons with a clean background to place bets or withdraw winnings on their behalf. During supervision, it is assessed whether the monitoring systems of gambling operators are capable of identifying situations where persons place large bets without a clear economic rationale or where winnings are distributed in an unusually frequent manner among specific persons.
- Third, supervision focuses on transaction structuring and the actual application of due diligence measures. It is assessed whether operators are able to identify related transactions designed to circumvent the 2,000-euro threshold and whether they will intervene in cases of suspicion even if the amounts involved are below the threshold. A key focus is on the substantive risk awareness of the organisation, in particular whether established procedures are merely formal or embedded in employees' day-to-day work. This requires staff to understand sector-specific risks, recognise

situations indicative of suspected money laundering and describe them appropriately. Low reporting activity in the context of growing market volumes indicates a need to strengthen employee awareness and the proper application of due diligence measures.

At the end of 2025, the Financial Intelligence Unit issued a compliance notice[19] to the sector to draw attention to:

- the identification of the threshold for applying due diligence measures (2,000 euros);
- the identification of suspicious gambling patterns;
- the identification of the origin of property and reporting of suspicious transactions to prevent the use of Estonian gambling operators for money laundering purposes.

Watch the Financial Intelligence Unit's EFIUC 2025 conference presentation on Malta's experience in the gambling sector

VIRTUAL CURRENCY SERVICE PROVIDERS

As of 31 December 2025, there were **36** valid authorisations for the provision of virtual currency services

2 supervision operations were carried out

This is the last Yearbook of the Financial Intelligence Unit in which we describe supervisory activities related to the virtual currency service provider sector.

The authorisations issued by the Financial Intelligence Unit for the provision of virtual currency services are valid until 30 June 2026 or until the company has obtained an authorisation of participant in markets in crypto-assets from the Financial Supervision Authority before that date. As of 1 July, the FIU will revoke all virtual currency service provider authorisations it has issued, and activities may thereafter be carried out only under an authorisation issued under the Market in Crypto-Assets Act. The Act transposes the European Union Markets in Crypto-Assets Regulation (MiCA).

According to the national risk assessment (2025), the level of money laundering risk and vulnerability among providers of virtual currency service is above average.

From 2021 to 2024, the supervisory focus of the Financial Intelligence Unit was largely directed at the virtual currency service provider sector, particularly in light of the risks associated with it. Supervisory proceedings carried out in 2025 in companies belonging to the two largest service providers once again highlighted deficiencies that had been identified previously.

Supervisory proceedings identified deficiencies in the management of risks related to money laundering, terrorist financing and financial sanctions, which may significantly reduce the effectiveness of due diligence measures:

- There was a lack of understanding of the risks associated with a customer that is a gambling operator. Crypto-asset companies do not always recognise that behind a single gambling service provider there may be thousands of end customers to whom services are effectively being provided. There is often insufficient insight into the risk profiles of these end customers and no ability to influence the due diligence measures applied to them, resulting in unclear allocation of responsibility and control. Moreover, there is insufficient assessment of whether and how prepared service providers are to take on, manage and mitigate the risks arising from such a business model. Practice shows that identifying more complex money laundering schemes can no longer rely solely on traditional know-your-customer measures. Increasingly, falsified documents and deepfakes are used to deceive online identity verification processes and online gaming platforms are used to create multi-layered money laundering schemes in which cryptocurrencies play an important role.
- Correspondent relationships are not always identified or assessed in line with their actual risk level. It is often not analysed whether the respondent institution applies adequate due diligence measures to its end customers or to what extent the correspondent institution itself should exercise control.
- When monitoring a business relationship, there is insufficient understanding of the customer's activities already at the time of establishment of the business relationship. Supervision revealed that if a virtual currency service provider lacks a clear overview of the purpose of the customer's business relationship, the customer's area of activity, expected transaction volumes and main contracting partners, it is impossible to form a complete picture of the customer. This, in turn, complicates the subsequent monitoring of the business relationship, including comparing the customer's actual transactions with previous forecasts, identifying suspicious transactions and reporting them to the Financial Intelligence Unit.

THE SCALE OF A BUSINESS RELATIONSHIP REQUIRES APPROPRIATE MONITORING

According to one virtual currency service provider, over a period of almost two years, they had nearly 500 legal person customers, a total turnover of over 15 billion euros and processed 700,000 transactions per day.

Supervisory findings showed that the company carried out insufficient monitoring of its customers and their transactions. This, in turn, indicated that the number of employees, their skills and their level of awareness may not be sufficient to mitigate the risks associated with the provision of services and to implement appropriate due diligence measures, including subsequent monitoring of transactions, which affects compliance with reporting obligations.

Under the Money Laundering and Terrorist Financing Prevention Act, providers of a virtual currency service must submit to the Financial Intelligence Unit an auditor's opinion on their own funds. The FIU issued compliance notices to 18 companies that failed to do so by the set deadline. Four service providers did not submit the report even after receiving a compliance notice and non-compliance levies were imposed on them.

FAILURE TO COMPLY WITH COMPLIANCE NOTICE RESULTED IN REVOCATION OF AUTHORISATION

In administrative case 3-22-1525, the Financial Intelligence Unit had revoked the authorisation of a virtual currency service provider because the undertaking had repeatedly failed to comply with the authority's compliance notices.

The circuit court of appeal noted that in the application of clause 2 of subsection 1 of § 75 of the Money Laundering and Terrorist Financing Prevention Act (revocation of an authorisation where the undertaking repeatedly fails to follow compliance notices issued by the FIU), it is irrelevant which statutory duty the Financial Intelligence Unit issued the compliance notice(s) to enforce. In reviewing the legality of the application of clause 2 of subsection 1 of § 75 of the Money Laundering and Terrorist Financing Prevention Act, it is neither necessary nor possible to retrospectively assess whether the appellant would have been able to provide information useful to the Financial Intelligence Unit by complying with the compliance notices. Knowledge that the appellant was no longer providing such services would have been equally informative regarding developments in the relevant sector requiring an authorisation and carrying a money laundering risk. For the performance of its AML/CFT duties, the Financial Intelligence Unit must have a comprehensive and detailed overview of developments in the sector, including any changes. The court further noted that, where an undertaking demonstrates a disregard for compliance with compliance notices issued by a supervisory authority, it is difficult to expect that it will exercise sufficient diligence in implementing necessary AML/CFT measures. In certain sectors, it is



justified, on the basis of a strong public interest, to expect a higher standard of due diligence from undertakings operating in those fields. The foregoing does not mean that the right of the Financial Intelligence Unit to request information from undertakings is unlimited in and of itself. However, once a valid compliance notice to provide information has been issued, the addressee must either comply with it or challenge it in the manner prescribed by law. The FIU correctly takes the view that where an authorised undertaking voluntarily refuses to provide information related to its activities which, in the opinion of the FIU, is necessary for the implementation of AML/CFT measures, including supervisory measures, it does not merit the level of trust required in a field of activity associated with such risks.

In conclusion, the court held that, as the appellant had failed to comply with three compliance notices issued by the Financial Intelligence Unit, this constituted a repeated breach. Consequently, the Financial Intelligence Unit legally revoked the authorisation.

Based on the deficiencies identified during supervision, the Financial Intelligence Unit has also considered it important to provide preventive support to market participants. To this end, targeted in-person trainings were held in 2025 at the premises of the Financial Intelligence Unit, focusing on practical supervisory observations. The trainings received positive feedback from participants and confirmed that effective prevention of money laundering and terrorist financing requires continuous dialogue, increased awareness and a risk-based approach.

Watch the Financial Intelligence Unit's EFIUC 2025 conference presentation on regulatory developments in the virtual currency service provider sector and the risks associated with nested services





ABOUT THE FINANCIAL INTELLIGENCE UNIT

Role

Financial intelligence units (FIUs) were established in 1996 in accordance with the global Financial Action Task Force (FATF) standards. The FATF was established to combat drug-related crime as a form of covert crime. By preventing money laundering, the objective was to curb the legalisation, ie laundering, of proceeds derived from drug-related crime and thereby reduce the incentive to commit such offences. The establishment of financial intelligence units was a central element of the new system, as it enabled the private sector to be more effectively involved in combating drug-related crime. In this context, private sector entities are required to know their customers and to identify suspicious or unusual transactions that may indicate the concealment of proceeds of crime. Such suspicions are then reported to the financial intelligence units.

According to the FATF standards still in force today, the cornerstone of the prevention system is an autonomous and independent financial intelligence unit. The FIUs receive suspicious transaction reports submitted by the private sector, analyse them and, where there are grounds to suspect a criminal offence, disseminate the information to investigative authorities. Such analysis is referred to as operational analysis. It is an activity in which existing and available information is used to identify specific targets, trace activities or transactions, and establish links between targets and potential proceeds of crime, money laundering, predicate offences and terrorist financing. FATF standards and European Union (EU) instruments provide that financial intelligence units must have the broadest possible access to financial, administrative and criminal information. This also includes the right to request bank account statements. This is also the case for EU financial intelligence units.

The anti-money laundering system has operated in this form worldwide for the past 30 years. The Egmont Group, a global umbrella organisation, comprises financial intelligence units from nearly 180 countries. More than 100 of these are administrative in nature. Other FIUs, which are attached to investigative authorities, also carry out their duties outside criminal proceedings. As part of an international assessment in 2016, it was found that a FIU in one country treated every analysis of information as the initiation of a criminal investigation; consequently, the FATF explained to that country that such a practice is not in line with the standard. As a result, that country received the lowest rating in the area concerning financial intelligence units.

In Estonia, the Financial Intelligence Unit was established in 1999 with the primary task of identifying money laundering and disseminating relevant information to investigators. Over the years, additional roles have been assigned to the Financial Intelligence Unit. Five years after its establishment, a supervisory function was added, followed by issuing authorisations in certain sectors, and subsequently the authority to act as a financial sanctions authority. Since 2021, when the FIU was established as a separate entity within the area of government of the Ministry of Finance, its responsibilities have expanded to include verifying information regarding the application of restrictions related to public procurement and suspected violations thereof, as well as providing input to foreign investment screening, among others. The obligation arising from the EU directive to designate the authority responsible for maintaining the beneficial ownership register is also planned to be assigned to the Financial Intelligence Unit in Estonia.

Therefore, a large number of the duties performed by the Estonian Financial Intelligence Unit are not related to its core function – the detection of money laundering, ie the conduct of operational analysis. The Financial Intelligence Unit has established clear data processing rules to protect the data collected using standardised methods and tools for the performance of its core function. Under these rules, data collected for the purpose of preventing money laundering is not used for supervisory purposes, and vice versa.

Given public interest in the powers of the Financial Intelligence Unit, it is necessary to explain both the functions of the FIU and the international standards and regulations underpinning them.

ISSUE OF REQUESTING BANK ACCOUNT STATEMENTS

According to the international standards of the Financial Action Task Force (FATF), financial intelligence units are a central part of a country's operational anti-money laundering and counter-terrorist financing network.

In order to detect money laundering and terrorist financing, the financial footprint of persons is analysed, which may include requesting bank account statements from credit institutions. This is common practice among financial intelligence units worldwide. In most cases, these involve covert criminal activity. This means that such activities do not have a victim or the victim does not report the offence. While drug-related crime was initially the primary focus, the scope was later expanded to include the prevention of terrorist financing, corruption, tax offences, human trafficking, fraud and other offences. The cases featured in the yearbooks of the Financial Intelligence Unit show that it is often the analysis of bank accounts that makes it possible to identify the necessary elements of a criminal offence, uncover money laundering schemes, restrict the transfer of assets suspected of being linked to criminal activity, and identify persons involved in violations of financial sanctions.

In the absence of the right to request bank account statements of suspects, the FIU is unable to perform its core function – the analysis of suspicions of money laundering.

Consequently, to perform its core function, the Financial Intelligence Unit has been requesting bank account statements in accordance with the law since 2000, including through mutual interpretation and co-operation between the parties. The same practice is followed in other countries as well.

In July 2025, the Chancellor of Justice published its position on the issue of information subject to banking secrecy. In its position of 29 September 2025, the Ministry of Finance confirmed the right of the Financial Intelligence Unit to request information subject to banking secrecy from credit institutions, including bank account statements. If the intention of the legislator had been to restrict the rights of the Financial Intelligence Unit in relation to bank account statements, such a restriction would have been explicitly set out in law. The Ministry of Finance has initiated amendments to the legislation concerning access to information subject to banking secrecy. As the drafter of the draft bill, the Ministry of Finance has noted that it does not entail any significant legal changes or other impacts.

The provisions of the Money Laundering and Terrorist Financing Prevention Act will be clarified in such a way that functions are clearly defined, specifying in which cases the Financial Intelligence Unit is entitled to request information subject to banking secrecy from credit institutions, both through the enforcement register and outside of it. Two separate draft bills also strengthen oversight of the Financial Intelligence Unit.

The broader objective of the draft bill is to restore confidence in rules that have been in force since 2000. At the same time, it is entirely understandable that the content and level of detail of bank account statements are not comparable

to those of 2000, when a large proportion of transactions were conducted in cash, living standards were lower and the ability to travel and use payment cards was not yet widespread.

At stake is nothing more and nothing less than the security of society – the state cannot prevent cross-border crime if it is excluded from international co-operation.

At the same time, it is important to bear in mind the core point described above – money laundering is, in most cases, a cross-border offence, which also gives its prevention an international dimension. However, international co-operation is based on the principle of reciprocity and mutual trust. For decades, co-operation between financial intelligence units has enabled the rapid and efficient exchange of financial information. Considering how quickly criminals move money, the importance of a rapid information channel cannot be overstated.

However, if the information shared remains incomplete or, in the worst-case scenario, responses to requests from foreign states cease altogether, the necessary information will not flow to us from other countries either.

In such a scenario, we would not only fail to prevent crime, but would in fact facilitate it – allowing criminals to enrich themselves at the expense of public assets and security, and to reinvest those proceeds into their own systems. This includes, for example, savings stolen from persons through telephone fraud, the financing of Russia's aggression through sanctions violations or influence operations aimed at distorting elections, as was the case in Moldova.

Read the full statement of the Financial Intelligence Unit on requesting bank account statements on our website (in Estonian)

We understand concerns that the system could be misused and that the data of persons who have not carried out any transfers or transactions indicative of criminal activity may be processed. We also recognise that, to provide reassurance, the system must have effective controls in place. To prevent misuse, the legislator has already established both internal and external security measures, but with joint proposals from the Ministry of Finance and the Financial Intelligence Unit, these controls will be further strengthened. We have, on our own initiative, proposed control measures in both draft bills amending the Money Laundering and Terrorist Financing Prevention Act, under which:

- the FIU will begin submitting annual reviews to the Security Authorities Surveillance Select Committee;
- the FIU will allocate permanent funding from its budget to the Estonian Data Protection Inspectorate, which will carry out regular inspections to verify the lawfulness of bank account requests;
- bank account requests made via the enforcement register will be made accessible to the relevant party after a certain period of time;
- everyone will have the right to contact the Estonian Data Protection Inspectorate at any time to verify the lawfulness of the processing of their data.

ORGANISATIONAL DEVELOPMENT AND IMPLEMENTATION OF STRATEGY

Compared to 2021, when the Financial Intelligence Unit was separated from the Police and Border Guard Board and established as an independent agency within the area of government of the Ministry of Finance, the organisation has grown in terms of the number of staff, internal procedures and professional expertise.

For the period 2022–2026, the Financial Intelligence Unit set three main strategic objectives:

- to serve as the national centre for the analysis of money laundering and terrorist financing risks in the Republic of Estonia and to guide risk management in the country;
- to implement smarter and more digitally advanced solutions and, where necessary, act as a leader in this field for both the public and private sectors;
- to serve as the centre of excellence for the prevention of money laundering and terrorist financing in the Republic of Estonia.

Over the past five years, there have been a number of developments in these areas, which have been documented in the yearbooks. A notable step forward has been the enhancement of case analysis capabilities in risk analysis. Although the results achieved with the contribution of the Financial Intelligence Unit often become apparent to the public only after 3–5 years, or in some cases even later, it is already evident that the volume of information provided to investigative authorities has increased.

The different forms of co-operation introduced with the public and private sectors have helped to better co-ordinate the activities of the parties involved. However, the development of the new information system has taken longer than expected and its impact can be assessed in the next strategic period.

Challenges to the principles underlying administrative confiscation, certain risk-based activities and the development of strategic analysis capabilities demonstrate that the field of anti-money laundering is keeping pace with societal developments. Legislative limits are established based on the circumstances prevailing at the time of their creation. However, society – in both its positive and negative aspects – is in constant change, which in turn drives discussions on the continued adequacy of legislative limits.

Disputes over freedoms and opportunities reflect societal development.

Strategic analysis is one of the core statutory functions assigned to the Financial Intelligence Unit. The FIU has continued this work using both existing and new tools. All analysis is based on data, yet at the time of the Danske Bank money laundering case, for example, such data was not available to the state.

Today, considerably more data is available, but challenges remain in relation to data quality and, above all, the legal basis for its analysis. To clarify the scope of the mandate granted to us, the Ministry of Finance submitted a draft bill for a round of approval already in 2024, with the aim of specifying whether and in which cases it is permissible to analyse combined datasets. In the summer of 2025, the Riigikogu passed the bill, but the President of the Republic did not promulgate it. At the time of preparing the yearbook, the draft bill was under renewed deliberation, ie processed for the second time.

The Financial Intelligence Unit has used digital solutions, for example, to support data-driven management. We have created data dashboards that provide structured data to the right people at the right time and in the appropriate format, in compliance with data processing rules. Management reports support the measurement of processes and the monitoring of trends.

We have taken a prudent approach to artificial intelligence (AI). First, needs were mapped and all employees were given the opportunity to submit proposals regarding the role of AI in day-to-day work. From several dozen ideas, a number were selected that were considered suitable for future implementation using AI. None of these involve the sharing of personal data with third parties. Work on the use of AI is still ongoing.

A cross-cutting activity throughout the entire strategic period has been the development of excellence both within the FIU and across the state as a whole. Operating as a centre of excellence is crucial, as success ultimately depends on the people who drive the development of these systems. We have made a conscious effort to ensure that the anti-money laundering system does not rely solely on the enthusiasm of a few persons, but rather that a high level of excellence forms a shared foundation across all institutions within the system.

As many as 24% of the employees of the FIU have obtained, or are in the process of obtaining, an international certification issued by the Association of Certified Anti-Money Laundering Specialists (ACAMS). Over the past five years, we have shared our experience and knowledge at nearly 160 information events, drawing on international expertise wherever possible. We have trained thousands of people from both the private and public sectors.

The expertise of the Financial Intelligence Unit has been extensively used in Estonia both in the MONEYVAL evaluation and in the preparation of the national risk assessment. Following both processes, action plans were drawn up under the leadership of the Ministry of Finance. For these plans to be successful, parties outside the area of government should also be interested in involving the FIU and, to some extent, this is already taking place. Society as

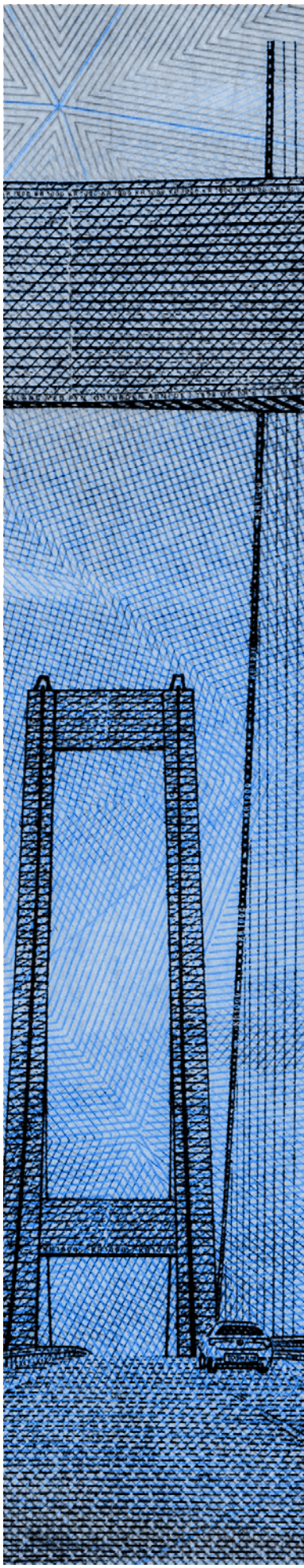


a whole benefits from the effective functioning of different institutions and well-informed opinions.

In countries where political will is lacking, the global umbrella organisation may sometimes need to set the tone. For this reason, meetings of the Egmont Group have been held, for example, in Malta and Latvia, which have been affected by money laundering scandals; in Armenia, Tanzania and Colombia, which face elevated money laundering risks; and in Barbados, Guernsey, Bermuda and Macau due to their offshore services sectors. It is to be hoped that Estonia will not require such attention.

The Financial Intelligence Unit has also shared its expertise internationally. There has been significant interest in our experience both in Europe and more broadly – particularly in the organisation of the virtual currency service provider market and in the analysis of risks related to crypto-assets.

A separate point worth highlighting is the shift towards co-operation with market participants, replacing an approach centred on coercive measures. As a result, both their anti-money laundering systems and the quality of data in national registers have improved.



"The Estonian Banking Association values the Financial Intelligence Unit as a partner in combating financial crime. Regular co-operation at both the council and committee levels of the Estonian Banking Association has helped to further strengthen risk awareness within the banking sector, and together we have developed a more effective framework for prevention and supervision. We appreciate the role of the Financial Intelligence Unit both as a strategic guide and as a promoter of practical co-operation in resolving complex cases and enhancing the professionalism of sector employees."

"The Estonian Service Industry Association has been co-operating with the Financial Intelligence Unit for several years. The co-operation is based on mutual respect and trust. The Financial Intelligence Unit is open to feedback and is genuinely interested in ensuring that service providers are kept up to date with the latest information and best practices."

"The Estonian Gaming Operator Association values its co-operation with the Financial Intelligence Unit and considers it to have become more meaningful and constructive over time. In recent years, mutual understanding has improved and the sector increasingly feels that its input is being taken into account."



Photo collage from the Financial Intelligence Unit's EFIUC 2025 conference, held from 3–5 November 2025.

"Co-operation between the Financial Intelligence Unit and the Chamber of Notaries has been practical and constructive. The Financial Intelligence Unit has been available to us both for day-to-day inquiries and requests, as well as during the conduct of the 2025 national risk assessment for the notarial sector, providing the necessary information, consultations and support. As a small organisation, we have particularly appreciated that the activities of the Financial Intelligence Unit are oriented towards finding practical solutions and developing a risk-based approach, including in the development of our supervisory methodology."

To ensure sustainability, a competency model has been developed for the Financial Intelligence Unit. It serves as a monitoring tool for immediate supervisors, a reference for employees and a resource for both career planning, recruitment and development decisions.

In addition to professional achievements, we also consider it important to support employees' mental health. The Financial Intelligence Unit has been recognised twice by Peaasi as a mental-health-friendly organisation: Bronze level in 2024 and the 'Blooming' label in 2025, equivalent to the Silver level awarded in the preceding year.

To support the next generation of professionals, the Financial Intelligence Unit provides internship opportunities, delivers a lecture course at the Estonian Academy of Security Sciences, and supports the onboarding of new employees in different ways. It may be useful for all actors in the field to note the experience of a candidate who applied for a position at the Financial Intelligence Unit, where despite strong qualifications and experience in anti-money laundering, they were unable to obtain employment in the field abroad in the early 2020s, as Estonia's reputation following a major money laundering scandal preceded them.

By learning from this experience, doing our utmost to combat money laundering, ensuring that current expertise is enhanced and shared, and supporting the next generation of professionals, the Financial Intelligence Unit continues to contribute to safeguarding the economic environment and financial system of Estonia.

Watch the Financial Intelligence Unit's EFIUC 2025 conference presentation on the role of financial intelligence units



FIVE YEARS IN NUMBERS

	2021	2022	2023	2024	2025
Total number of reports	16 655	14 920	12 500	14 185	14 323
incl reports concerning money laundering suspicion	14 064	11 637	9 635	10 366	10 443
terrorist financing	303	312	273	174	138
sanctions	99	953	606	593	455
Disseminations					
Analysed disseminations to Estonian investigative authorities	287	134	150	133	147
Spontaneous disseminations and inquiries to foreign countries	222	246	225	261	232
Received spontaneous disseminations and inquiries from foreign countries	673	562	552	515	589
Restrictions on disposal[5]					
Number of 30-day restrictions	15	57	28	17	6
value of assets	2.22 million euros	16.4 million euros	4.37 million euros	7 million euros	124 000 euros
Number of 60-day restrictions	20	12	50	9	2
value of assets	2.23 million euros	9.34 million euros	9.45 million euros	6.6 million euros	14 000 euros
Number of 365-day restrictions	5	5	35	1	0
value of assets	20 000 euros	1.44 million euros	3.85 million euros	1.1 million euros	0 euros
Number of compliance notices to transfer property to state revenue	0	2	10	19	3
value of assets	0	80 000 euros	1.36 million euros	470 000 euros	18 200 euros

[5] The information on disposal restrictions for 2022 has been corrected following the publication of the yearbook in 2023.

Money laundering convictions	4	4	4	4	5
Total value of confiscated assets[6]	1.36 million euros	2.38 million euros	2.43 million euros	4.1 million euros	6 million euros
Amount of funds frozen under financial sanctions[7] as of 31 December	1 079 euros	20 million euros	33 million euros	50 million euros	46 million euros
Not made available[8]	29 068 euros	24 million euros	59 338 euros	34 000 euros	220 000 euros
Application of a deposit limit[9]	-	425 156 euros	197 530 euros	353 000 euros	436 820 euros
Authorisations[10]	1345	1007	872	744	678
Virtual currency service provider[11]	478	148	53	42	36
Providers of trust and company services	326	321	277	259	229
Financial institution	325	324	329	248	227
Pawnbrokers	114	112	113	101	98
Buying-in and wholesale of precious metals and stones	102	102	100	94	88
Gambling operator[12]	26	28	34	42	58
Supervisory activities (completed as of 31 December)					
On-site	32	4	4	14	7
Off-site inspections	20	0	0	0	11
Information and training events held	17	18	34	49	35
Number of participants	1147	2371	5025	5568	2812

[6] All confiscated criminal proceeds regardless of the crime. (Prosecutor's Office Yearbooks 2021 to 2025).

[7] The movement, transfer, alteration, use, access, or dealing with restricted funds in any way that would result in any change in their volume, amount, location, ownership, possession, character, destination or other change that would enable the funds to be used, including portfolio management.

[8] Transactions or operations refused under financial sanctions, in the corresponding total amount.

[9] The financial sanction introduced in 2022 prohibits the acceptance of deposits exceeding EUR 100,000 from Russian citizens, natural persons residing in Russia, legal persons, entities and bodies established in Russia, as well as legal persons, entities or bodies established outside the EU in which more than 50% of the ownership rights are held by Russian citizens or natural persons residing in Russia.

[10] The number of valid authorisations issued by the FIU as of 31 December.

[11] Until the end of 2022, one company could have several different authorisations for the provision of different virtual currency services.

[12] The authorisation is issued by the Tax and Customs Board.

REFERENCES AND FURTHER READING

[1] Estonian Ministry of Finance. (2025). The Estonian National Risk Assessment Report in the Field of Money Laundering for the Years 2020–2024. https://www.fin.ee/sites/default/files/documents/2025-12/NRA%202025%20ML%20Report_ENG_18.12.pdf

[2] U.S. Attorney's Office, Western District of Washington. Two Estonian fraud defendants sentenced for $577 million fraud scheme. 12.08.2025. https://www.justice.gov/usao-wdwa/pr/two-estonian-fraud-defendants-sentenced-577-million-fraud-scheme

[3] Estonian Ministry of Finance. (2025). Estonian National Risk Assessment Report on Countering Terrorist Financing 2020–2024. https://www.fin.ee/sites/default/files/documents/2025-12/NRA%202025%20TF%20Report_ENG_17.12.pdf

[4] European Commission. (2020). Commission Opinion, 19.6.2020, on Article 2 of Council Regulation (EU) No 269/2014 (C(2020) 4117 final). https://finance.ec.europa.eu/document/download/320cea0c-2f2e-4337-827e-d55b1080dc05_en?filename=200619-opinion-financial-sanctions_en.pdf

[5] European Commission. (2026). Frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it (consolidated version). https://finance.ec.europa.eu/document/download/66e8fd7d-8057-4b9b-96c2-5e54bf573cd1_en?filename=faqs-sanctions-russia-consolidated_en.pdf

[6] Financial Action Task Force. (2025). Complex proliferation financing and sanctions evasion schemes. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf

[7] Estonian Ministry of Finance. (2025). The Estonian National Risk Assessment Report in the Field of Financing the Proliferation of Weapons of Mass Destruction for the Years 2020–2024. https://www.fin.ee/sites/default/files/documents/2025-12/NRA%202025%20PF%20Report_ENG_19.12.pdf

[8] European Gaming and Betting Association. Gambling Market Share (2019-2029). 25.03.2025. https://www.egba.eu/resource-post/gambling-market-share-2019-2029/

[9] Egmont Group of Financial Intelligence Units. Annual Report 2020/2021. https://egmontgroup.org/wp-content/uploads/2022/10/EGMONT_21-267_2020%E2%80%932021_AR-E_WEB.pdf

ANALYSES PUBLISHED BY THE FINANCIAL INTELLIGENCE UNIT IN 2025

[10] Feedback from the Financial Intelligence Unit on obliged entities' compliance with the reporting obligation in 2024 (April 2025, in Estonian) .
https://fiu.ee/juhendid-analuusid-ja-materjalid/tagasiside-teatajatele#tagasiside-de-virtuaalv--2

[11] Nested Services in Virtual Currency Exchanges (December 2025) .
https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#nested-services-in-v

[12] Indicators of Terrorist Financing Risks Related to Non-Profit Organisations and Measures to Mitigate those Risks. (December 2025, in Estonian) .
https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#vabauhendustega-seot

GUIDELINES PUBLISHED OR UPDATED BY THE FINANCIAL INTELLIGENCE UNIT IN 2025

[13] Obligations of virtual currency service providers in correspondent relationships (March 2025) .
https://fiu.ee/en/guidelines-fiu/guidelines#obligations-of-virtu

[14] Reporting templates for persons subject to special obligations: report on movements of funds in frozen accounts / report on frozen funds and economic resources held by a person subject to special obligations (April 2025, in Estonian).
https://fiu.ee/oigusaktid-ja-juhendid/juhendid#erikohustustega-isik

[15] Guidelines of the Financial Intelligence Unit for the application of financial sanctions (June 2025, in Estonian).
https://fiu.ee/oigusaktid-ja-juhendid/juhendid#rahapesu-andmeburoo-

[16] Guidelines for persons with special obligations supervised by the Financial Intelligence Unit (June 2025) .
https://fiu.ee/en/guidelines-fiu/guidelines#guidelines-for-perso

COMPLIANCE NOTICES PUBLISHED BY THE FINANCIAL INTELLIGENCE UNIT IN 2025

[17] Compliance notice for providers of company services (March 2025, in Estonian) .
https://fiu.ee/uudised/margukiri-usaldushalduse-ja-ariuhingute-teenuse-pakkujatele

[18] Compliance notice for providers of company services (December 2025, in Estonian) .
https://fiu.ee/uudised/margukiri-usaldushalduse-ja-ariuhingute-teenuse-pakkujatele-0

[19] Compliance notice for gambling operators (December 2025, in Estonian) .
https://fiu.ee/uudised/margukiri-hasartmangusektori-teenusepakkujatele

Guardian of honest financial transactions

Send us a tip!

Anonymous tips that can help prevent money laundering, terrorist financing or the evasion of financial sanctions can be submitted to the Financial Intelligence Unit via email at *vihje@fiu.ee* or by completing the online form *fiu.ee/vihjeliin*

Sending a tip does not absolve obliged persons of their reporting obligation