Republic of Estonia
Financial Intelligence Unit

Estonian Financial Intelligence Unit Yearbook 2023

Estonian Financial Intelligence Unit Yearbook 2023

Copy editor: Mare Timian
Translation: Transly Translation Agency
Designed by: Identity OÜ
Cover photo: collage from photos by Eesti Pank
Illustrations: Shutterstock

The Financial Intelligence Unit
Pronksi 12, 10117 Tallinn

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

CONTENTS

Photo: Jarek Jõepera

Dear reader!

The 2023 yearbook of the Estonian Financial Intelligence Unit is in front of you!

The Financial Intelligence Unit (FIU) will celebrate its 25th anniversary on 1 July 2024. Year after year, criminal offenders are becoming more sophisticated, but there is no doubt that we at the FIU can keep pace, and in some respects, we are even ahead of them. You can read about our significant progress and ambitious goals below.

At the beginning of 2023, a report compiled by the Committee of Experts of the Council of Europe MONEYVAL was published, describing Estonia's positive developments and shortcomings in combating money laundering and terrorist financing on more than 300 pages. The report provided a consolidated evaluation of the last seven years, but our current activities are already the subject of the next evaluation, leaving no time or space to rest. For this reason, we have to work together as a country because we are only as strong as our weakest link. On 1 January 2021, the FIU became an autonomous and independent government agency under the jurisdiction of the Ministry of Finance. With this change, the resources of the FIU increased exponentially. As of the end of 2023, we can say that recruitment is essentially complete and we are close to operating at full capacity. These activities have already yielded good results in terms of both implementing financial sanctions and exercising supervision, in particular in the sector of virtual asset service providers. However, the functions mentioned above are duties that only a few of the world's more than 170 financial intelligence units undertake. Therefore, we must carefully consider when assigning the FIU additional new duties that do not align with its core function. In this way, the focus may be shifted away from areas for which financial intelligence units were established: the collection and analysis of information on suspected money laundering and its transmission to investigative authorities.

Over the next few years, as also pointed out by MONEYVAL in its report, we will thus need to focus more on the quality of the information that reaches

the FIU and on encouraging investigative authorities to use our products even more. To deliver even better results, we expect market participants to inform us about transactions happening in real-time, rather than those from years ago. In the case of the latter, both the laundered money and the criminal offenders themselves have already vanished.

In the case of delay, both the laundered money and the criminal offenders involved will be lost.

The FIU itself also has significant room for improvement: it is certainly unsatisfactory that only 11 new criminal proceedings were initiated out of approximately 150 disclosures. As a state, we must also seriously consider whether we can indefinitely shut down new channels in the private sector or whether we should use real prison sentences and the confiscation of assets as a means of sanctioning criminal offenders. Last year, no sentences of imprisonment were imposed for money laundering.

The FIU has been granted by law the right to confiscate assets through administrative confiscation. We used this right more actively in 2022 and 2023. At the same time, we have critically assessed all the circumstances of each case in order to be sure of the content of the case and not violate the rights of the possessors of the assets. It is not a procedure where we determine someone's guilt under criminal law; rather, the objective is to confiscate assets from persons who, all things considered, do not own them. The FIU is an agency that deals with risks and operates based on its own clear conscience and the principle of #lawfulassets. Such a right of confiscation is not unique in the world; it is being implemented in more and more countries precisely because detecting the original crime has become so challenging in an ever-globalising world that alternative measures have to be used. We are likely to witness the movement of criminal assets that have remained at a standstill for years, waiting to 'get out', whether this means assets related to the theft from the three

Assets that have been dormant for years come to light and can be confiscated.

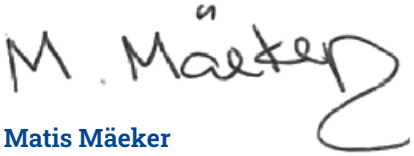
Moldovan banks in 2014 or assets from other cases that we are all familiar with. As a new risk, Estonian residents seek to transfer their assets to Lithuania for the purposes of tax evasion or in connection with other offences, with the intention of withdrawing them in Estonia in cash. Cheats will be caught and provided with feedback on their actions.

Last year, for the first time in recent history, we also restricted virtual asset transactions suspected of being linked to terrorist financing. This once again highlights how open the Estonian economic space is to cross-border crime. For this reason, we have decided to contribute to different international working groups and joint analyses. While we have already published a form of cooperation on the Israel-Hamas war, there are additional similar forums underway in the background. These formats allow us to better focus our analyses and find potential criminal offenders.

Investigative journalism also plays a valuable role in uncovering and exposing cheats. For instance, a series of articles about Estonian virtual asset service providers was published in Estonia in autumn 2023, highlighting the same risks and the same world that the signatory addressed in an interview with the media in October 2021. An observant reader must have noticed that the series of articles only provided examples of frauds and their victims. However, in addition to fraud, we also encountered drug-related crime, child pornography, organised crime and much more. This was not surprising, considering that just a few years ago, unofficial statistics suggested that Estonia was home to nearly 55% of the world's virtual asset service providers. Now, the share of Estonian authorisations is just over 2%. At a time when approximately 600 companies still held authorisations in Estonia, the FIU had at least one item of negative information related to money laundering on around 95% of the service providers or persons related to them. While there were no surprises for us this time in the articles reported by the media, the diligent work of journalists can sometimes provide valuable insights for us.

We have experienced two major money laundering crises in Estonia: first in the banking sector and now in the sector of virtual asset service providers. We are working to prevent the occurrence of another one. We are in the process of developing a strategic analysis function or, as we call it, SAF, which could filter out new trends and typologies from mass data, as well as individual cases exhibiting unusual transaction patterns between parties.

At the FIU, we are guided by our vision every day: 'A step ahead in monitoring the integrity of financial transactions.'



Matis Mäeker
Head of the Estonian Financial Intelligence Unit

2023 timeline

JANUARY

- Information on unauthorised company service providers was forwarded to the Police and Border Guard Board for processing
- The MONEYVAL evaluation report on Estonia was published on 27 January

MARCH

- The FIU held an international three-day conference along with training on confiscation for judges and investigators
- On 1 March, the Organisational Supervision Department and Communication and Cooperation Department were added to the structure of the FIU

APRIL

- The FIU provided feedback to market participants on low reporting activity

MAY

- There were 100 valid authorisations in Estonia for the provision of virtual asset services, compared to the nearly 500 in March 2022 when new statutory requirements entered into force
- A non-compliance levy was imposed on 45 company service providers for failure to provide data
- The FIU published the typology of trade-based money laundering and an overview of sanctions evasion through the use of virtual assets
- The Markets in Crypto-Assets (MiCA) Regulation of the European Union (EU) entered into force

JUNE

- The FIU's study on the use of cash indicated a higher risk of money laundering in the paying agents, real estate, foreign exchange, investment gold and gambling service sectors
- A 17-member committee led by Matis Mäeker submitted 15 proposals to the AML/CFT Governmental Committee to improve the effectiveness of the country's AML/CFT system

JULY

- Indicative guidelines for undertakings to detect circumvention of sanctions were published by the competent authorities of Estonia, Latvia, Lithuania and Poland

AUGUST

- A joint study conducted by the Estonian, Latvian and Lithuanian FIUs revealed a decrease in cash inflows from Russia and a significant outflow from the EU, in Estonia's case to the United Kingdom

SEPTEMBER

- The FIU published a typology notice on the use of payment cards to circumvent sanctions
- IMF report on the fight against money laundering in the Nordic and Baltic countries acknowledged the efforts made
- Regular reporting obligation was imposed on virtual asset service providers as of 2023
- The authorisations of 13 company service providers who repeatedly failed to comply with supervision compliance notices were revoked

NOVEMBER

- The FIU published an overview of the financing models of the terrorist organisation Hamas
- The FIU joined the international CTFTI task force to enhance measures aimed at preventing the financing of terrorism

DECEMBER

- The EU adopted the 12th package of sanctions, including a ban on Russian nationals owning and managing companies providing virtual asset services
- With the support of the United States Department of State, sanctions training was provided to nearly 80 participants from the private and public sectors
- The technical assistance project of the United States aiming to raise the skills and knowledge of responsible authorities in Estonia ended
- Matis Mäeker was elected Vice-Chair of the MONEYVAL Bureau

Prevention of money laundering

Money laundering risk profile

MONEY LAUNDERING RISK LEVEL IN ESTONIA 2023: MEDIUM

PLACEMENT → **LAYERING** → **INTEGRATION**

Cross-border money laundering vs laundering of assets derived from criminal activity: cross-border money laundering predominates significantly

Sectors with above average risk: credit institutions, virtual asset and company service providers

Vulnerable sectors: a very small number of credit institutions, virtual asset and company service providers

Main predicate offences: fraud, circumvention of sanctions, tax offences

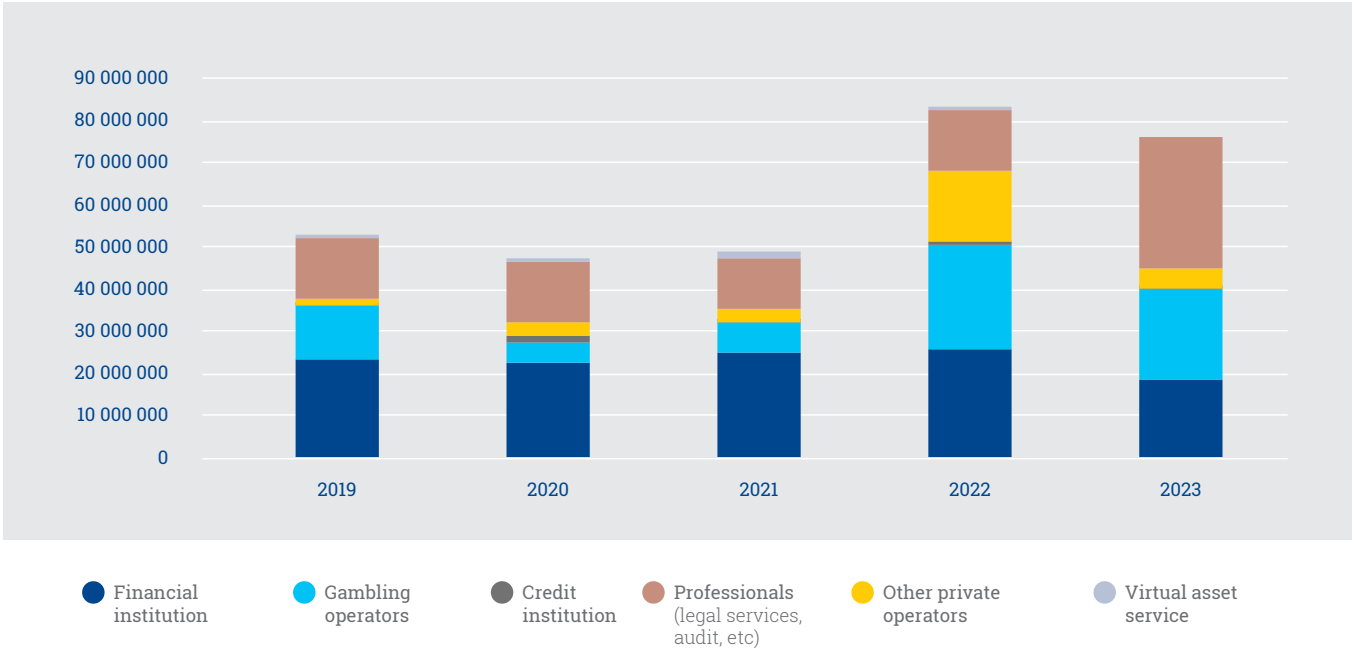
ESTONIA IS MORE INVOLVED IN CROSS-BORDER MONEY LAUNDERING IN THE LAYERING PHASE

The risk of cross-border money laundering remains significantly higher in Estonia compared to the domestic risk, which is why the greatest threat to Estonia is the layering of foreign proceeds of crime through Estonia. While the cases analysed in 2022 also indicated a certain level of integration of criminal proceeds into real estate, the decrease in eastbound cash flows in 2023 resulted in less integration of criminal proceeds into the real estate sector.

Estonia is linked to cross-border money laundering through accounts opened here (including virtual bank accounts, or VIBANs, opened by respondent institutions for payment and e-money institution customers), wallets opened by virtual asset service providers and legal persons established in Estonia that are used in other countries for the purpose of criminal money laundering (tax, investment, e-commerce and other fraud). These findings are derived from both the external inquires of the FIU, international exchanges of information between investigative authorities and requests for legal aid. This indicates that credit institutions, virtual asset and company service providers are still sectors with a higher than average risk and those most vulnerable, with the first two being associated with accounts or wallets located in Estonia and the latter with the exploitation of companies established in Estonia in foreign countries.

When it comes to money laundering in Estonia, greater attention should be paid to cash as a means of payment. Despite the rise of electronic payment methods and new technologies, criminal offenders still favour cash as their preferred payment method. Cash transactions in Estonia have picked up again after the decline in 2020–2021. The surge in large cash transactions has also increased the money laundering risk of a number of cash-intensive services, including foreign exchange, investment gold sales and gambling services. Systemic large-scale cash transactions indicate a potential increased risk of money laundering associated with economic and other criminal activities. Nearly four times more cross-border cash transactions are reported in the incoming direction to Estonia than in the outgoing direction.

AMOUNTS RELATED TO CASH REPORTS FROM OBLIGED SECTORS (IN EUROS)

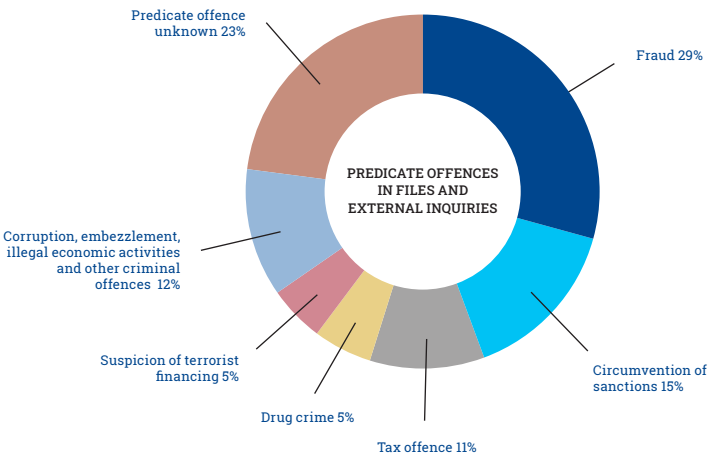


PREDOMINANCE OF FRAUD AS A PREDICATE OFFENCE AND CIRCUMVENTION OF SANCTIONS

Based on the cases analysed by the FIU and information from other law enforcement authorities, fraud continues to be the most common predicate offence for money laundering. Their connection to Estonia involves transferring the proceeds resulting from the fraud to an account of an Estonian credit institution.

In 2023, fraud cases experienced a decrease in risks related to virtual asset service providers. A large number of foreign inquiries were related to service providers who were no longer authorised in Estonia.

Frauds are not exclusive to Estonia, they have increased massively worldwide. The European Financial and Economic Crime Centre (EFECC) at Europol has also observed an increase in online fraud and the diversification of fraud types.



In addition to fraud, albeit to a much lesser extent, the cases analysed by the FIU also identified tax and drug offences and suspicions of illegal economic activities, embezzlement and corruption as predicate offences for money laundering. Such criminal offences are investigated by investigative authorities, but in most cases they are not linked to subsequent money laundering.

Russia's war of aggression in Ukraine has significantly increased the circumvention of sanctions among predicate offences for money laundering. Cases related to the circumvention of financial sanctions were much more prevalent at the FIU in 2023 compared to previous years. Another risk involves the intertwining of sanctions circumvention and money laundering.

The graph shown has two unknown variables, as a result of which it is not possible to draw any conclusions regarding either the predicate offences or their extent.

The first variable pertains to the limited knowledge Estonia has regarding the amount of criminal assets originating from Russia that reach Estonia through other countries, including EU countries, due to the political situation in Russia. Russian law enforcement authorities are either cut off from information-sharing channels or have no interest in investigating from which Russian criminal offences and to what extent funds reach other countries. As a result, it is not possible to identify or distinguish funds derived from corruption, tax offences or other criminal offences that have likely passed through the Estonian economic space in one way or another and at least to some extent. Therefore, increased attention needs to be directed towards implementing due diligence measures on funds originating from Russia-friendly countries.

Another blind spot to consider is the concentration of payment institutions holding authorisations from different countries in Lithuania, from which cash flows have increased over time, yet their origin and associated criminal offences remain unknown. In addition to cash flows from Lithuania to Estonia, the FIU has observed in cash reports a typology of 'cashing' where paying agents of Lithuanian e-money or payment service providers in Estonia are used to withdraw or deposit the funds in cash. This means that Estonian residents, including legal persons, use accounts opened with foreign payment intermediaries. However, to obscure the trail of assets, they withdraw the funds through an agent located in Estonia.

CROSS-BORDER MONEY LAUNDERING INVOLVES COUNTRIES CLOSE TO ESTONIA, CENTRAL ASIAN AND SOME OTHER INDIVIDUAL COUNTRIES

The information exchanged with foreign countries, received reports and payment and virtual asset flows show that Estonia's cross-border money laundering risks are primarily associated with Lithuania (a wide range of criminal offences), Latvia and Finland (tax and other criminal offences) as well as Turkey, the United Arab Emirates, Hong Kong and Central Asian countries (criminal and sanctions offences stemming from Russia).

While the latter has been the subject of several studies published by the FIU as well as a wide range of typology papers published in Europe and G7 countries, money laundering related to Latvia and Finland is linked to Estonia's closer commercial ties with these countries. As mentioned earlier, the risks stemming from Lithuania are of an unknown magnitude and we have also referred to them in previous yearbooks. This year, we will look at this risk in greater detail.

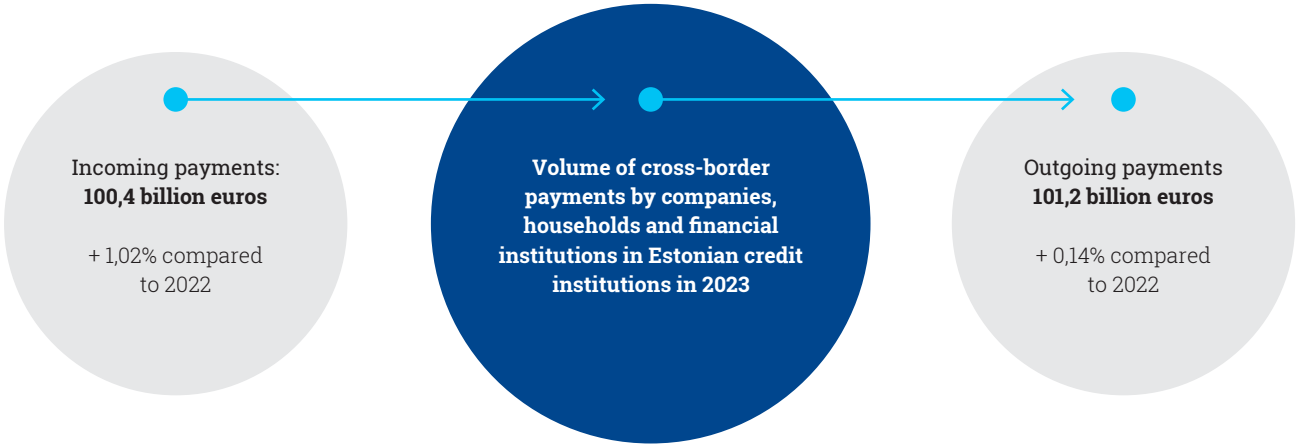
In 2023, goods and services worth nearly 2.6 billion euros were exported from Estonia to Lithuania. At the same time, a total of 19.3 billion euros were deposited to the bank accounts of Estonian credit institutions from Lithuania. Although these values cannot be compared one-to-one (as money could have been received from tourists with a payment account in a Lithuanian financial institution, etc), such a stark discrepancy in the figures suggests that the received cash flow is not, to a very large extent, justifiable by general economic relations. Lithuania has positioned itself as a fintech-friendly country, which has resulted in a number of payment and e-money institutions as well as virtual asset service providers obtaining authorisations. The reporting obligation of the Lithuanian private sector has surged due to the growth of the aforementioned fintech companies. However, the Lithuanian FIU considers that the level of compliance with the reporting obligation is still too low in certain high-risk sectors.

In the autumn of 2023, the IMF published a report on the dynamics and risks of cash flows in the Nordic-Baltic region illustrating the risks that Lithuanian financial flows are related to and which, to some extent, therefore also find their way to Estonian economic space. According to the report, Lithuanian financial flows are related to non-resident customers and, as of 2020, the volume of transactions has increased sharply, which deviates from the usual economic pattern. The volume of such transactions in Lithuania accounts for 13.3% of all transactions (in Estonia, the same figure is 2.3%). According to the IMF report, the increase in payment volumes is attributed to transactions with financial centres such as Switzerland, Hong Kong, Singapore, United Arab Emirates, Gibraltar, Isle of Man, Liechtenstein and Jersey. Despite the fact that this image of Lithuania shows the severity of the risks, the report did not account for all transactions of Lithuanian payment intermediaries. The above indicates that the actual extent of the risks associated with Lithuania is greater than is currently known and that above-average attention must be paid to these transactions.

[1] These include accounts opened in Estonian credit institutions for natural and legal persons and financial institutions (excluding credit institutions).

CREDIT INSTITUTIONS, VIRTUAL ASSET AND COMPANY SERVICE PROVIDERS ARE STILL THE MOST-AT-RISK AND MOST VULNERABLE SECTORS

As noted above, the most common link or threat is the movement of funds obtained through fraud from foreign persons to accounts in Estonia. Examples include accounts opened in Estonian credit institutions primarily for financial institutions in foreign countries whose customers, in turn, use a final-stage service, ie virtual bank accounts (VIBANs). Internationally, it is well known that in situations where criminal offenders actively use certain accounts or service providers to commit fraud, these accounts are also used to transfer funds derived from other criminal offences. In terms of vulnerability, the level of the reporting obligation of at least one credit institution is still not estimated to be sufficient and, at the same time, their risk appetite in serving customers was higher in 2023 than what the risk controls would have allowed.



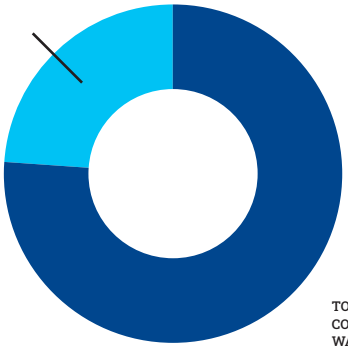
Different sanctions circumventions are also primarily related to credit institutions. All of this means that, considering the overall volume and trends of payments (see information on risky countries above), the risk of money laundering associated with credit institutions remains moderate.

As a result of streamlining of the sector, the number of virtual asset service providers has decreased sevenfold compared to the past, with 53 authorisations remaining, which has led to a reduction in the overall volume of risks. If in 2021 the volume of transactions by virtual asset service providers converted to euros was around €20 billion and in 2022 around €10 billion, then by 2023 the volume had risen again to €20 billion. Although the volume of transactions has not decreased in absolute terms, there has been a decrease in the number of external inquiries concerning virtual asset service providers, as well as a reduction in the number of references found in public forums regarding Estonian service providers operating illegally. At the same time, companies that were once authorised to operate in Estonia, but now have no connection with the country other than a private limited company in the commercial register, but who continue to advertise themselves as Estonian service providers while mediating crimes, pose a significant challenge to the reputation of the Estonian state. Currently, there are no mechanisms in place in Estonia to stop and prosecute these service providers. The reports submitted by virtual asset service providers indicate a more serious approach to due diligence measures than in the past. Nevertheless, in addition to the above, the risk of money laundering in the sector remains significant for several reasons. During the year, less than half of market participants sent reports to the FIU. Undertakings also exhibit shortcomings in risk assessment: risk assessment and risk appetite documents are not in line with reality and there are problems with customer identification. Some transactions conducted by Estonian service providers are associated with high-risk platforms. Virtual asset flows continue to be associated with criminal activity, mainly fraud in Estonia. As a result of the above, both the risk and vulnerability associated with the sector remain relevant, with the overall risk assessment being medium.

The risk of company service providers is increased by the cases identified by the FIU where the company service providers do not implement due diligence measures when serving customers classified as high-risk, suspected of money laundering or subject to sanctions, and have failed to perform their reporting obligation. Nearly two-thirds of company service providers provide company services to non-residents, which is why it is unsatisfactory that only 4% of these service providers submitted reports in 2023. Many companies offer accounting and consulting services to their customers in addition to company services. Often, these service providers have a small number of employees, even in the case of high-turnover businesses, which poses a risk that they may not be able to implement anti-money laundering due diligence measures to the required extent.

In addition to the above, the above-average risk, the vulnerability of the sector and thus the medium risk level are caused by the fact that companies associated with Estonia are used for criminal purposes in other countries, some of which are established by or linked to company service providers. One-third of the foreign inquiries submitted to the FIU involve legal persons registered in Estonia. Nearly half of the Estonian companies associated with foreigners have no active economic activity in Estonia.

Turnover attributed to company services in 2023:
25 million euros



TOTAL TURNOVER OF COMPANY SERVICE PROVIDERS WAS 80 MILLION EUROS ACCORDING TO RESPONSES TO FIU QUESTIONNAIRE

Money laundering convictions

In 2023, four county court judgments convicting 14 people of money laundering entered into force in Estonia. All cases were resolved through a compromise procedure in court and none of the accused received an actual prison sentence.

Assets with a total value of more than 668,000 euros and 37,000 United States dollars, along with 480 British pounds, were confiscated based on the judgments.

The common thread in all three cases was the commission of business email compromise (BEC) fraud as the predicate offence for money laundering. In such a case, the criminal offender has obtained email addresses and telephone numbers that resemble the originals as closely as possible, and as a result of the fraud, the victims unknowingly and mistakenly transfer money to the criminal offender's account.

In the cases that resulted in a conviction, the FIU cooperated with the investigative authority and shared information for the detection, prevention and pre-trial investigation of the criminal offence. In three of the cases, the FIU submitted a report of a criminal offence to the police and imposed restrictions on criminal assets, which were later seized during criminal proceedings.

In all cases, the convicted persons aimed to conceal the illicit origin of the money, their connection to it and to integrate the funds into the legal economic circuit.

CASE 1-23-250

The convicted persons acted jointly. The funds obtained had been fraudulently acquired from foreign companies and deposited into the bank accounts of different companies as a result of the fraud, which were in turn transferred to other bank accounts. The convicted persons registered companies in their own names and opened bank accounts with the intention of concealing the origin of assets and conducting transactions involving the assets subject to money laundering.

The bank account details, along with the ID card and passwords, as well as the bank documents were transferred to third parties, allowing them to conduct transactions on the bank account of the private limited company. In addition, the objective of the convicted person in acting jointly was to find persons willing to register companies in their names in Estonia and to open bank accounts for these companies. In doing so, the persons involved in the criminal scheme aimed to make cash settlements through the established companies. The funds previously obtained through the BEC fraud from foreign companies were transferred to the bank accounts of companies and legal persons operating in the UK, the USA and Estonia.

CASES 1-23-654, 1-22-7510 AND 1-22-7110

The convicted persons acted on the instructions of an unidentified person in one case and a Nigerian citizen living in Slovakia in other cases. The objective was to conceal the illicit origin of the funds and the connection between the criminal offenders through different activities.

The convicted persons allowed a third person to transfer funds to their company and personal accounts, which had been previously obtained through BEC fraud from companies operating abroad.

The aim of the criminal scheme was to transfer funds, including through fictitious contracts, to the bank accounts of different legal and natural persons acting as fronts or to withdraw cash from ATMs.

Cooperation in the prevention of money laundering

150

disclosures were filed with investigative authorities concerning 230 reports

Received

552

foreign inquiries and spontaneous disclosures

Submitted

225

foreign inquiries and spontaneous disclosures

Investigative authorities play a key role in bringing money laundering cases to court. The disclosures of the FIU support the work of investigative authorities in the detection, prevention and pre-trial investigation of criminal offences. The volume of information forwarded to investigative authorities increased to 150 disclosures in a year, the majority of which comprised spontaneous disclosures and reports of criminal offences. In a quarter of cases, information was forwarded in connection with an ongoing criminal case. In addition, on the basis of 1,352 reports, information on suspicious activities as well as on potential criminal assets was promptly shared with investigative authorities on 610 occasions.

Based on the disclosures of the FIU, 11 criminal proceedings were initiated in 2023, with most of them related to predicate offences for money laundering and three cases based on the elements of money laundering.

The content of the disclosures is a reflection of the risk profile of the FIU: the information most frequently identified and forwarded concerned money laundering, fraud (mainly investment fraud), tax offences and suspicions of sanctions circumvention.

The FIU also has a mandate to cooperate with other competent authorities to prevent money laundering and terrorist financing or related criminal offences and to fulfil the tasks of the supervisory authority arising from the law.

As part of this cooperation, the FIU forwarded information to:

the Tax and Customs Board regarding applications for authorisation to organise gambling on 25 occasions;

the Police and Border Guard Board regarding the processing of digital identity cards for e-residents and temporary residence permits for major investors for business purposes on approximately 10 occasions;

the Financial Supervision Authority regarding the processing of authorisations on 17 occasions;

the Foreign Investment Committee at the Consumer Protection and Technical Regulatory Authority regarding the assessment of the reliability of foreign investments as of September 2023. The FIU was tasked with reviewing 158 reports and applications and, where necessary, conducting background checks.

In the framework of the institutional form of cooperation established under the auspices of the FIU, cases related to the Russian military aggression in Ukraine and the inadequate application of due diligence measures to prevent fraud were addressed. The FIU also prepared a national PPP (Public-Private Partnership) project together with five of Estonia's largest banks to actively contribute to the identification and sharing of cases and typologies.

International cooperation in money laundering matters involves both direct communication with national FIUs and participation in different organisations, working groups, task forces and projects.

Foreign inquiries received from other FIUs still largely concern respondent accounts opened in Estonian credit institutions, but also companies registered in Estonia that were involved in suspected money laundering transactions abroad and did not operate or have a permanent establishment in Estonia. These companies are often not registered as persons liable to value added tax, have failed to submit their annual reports on time or the transactions reported in the inquiries are significantly higher than the sales revenue recognised in the annual reports. This indicates cases where companies registered in Estonia are used to commit tax offences abroad, which may also involve other violations. A total of 16% of foreign inquiries were related to Estonian e-residents, including those whose status has expired, which is similar to the figure of the previous year.

The nature of foreign inquiries also requires increased attention to be paid to e-commerce in the future. Foreign inquiries indicate a growing trend of exploitation of Estonian companies in different e-commerce frauds where merchants operating under the guise of Estonian companies deceive customers with misleading product descriptions and deliver goods of significantly lower value than advertised or fail to deliver the goods altogether. As indicated by the money laundering risk profile, many Estonian persons and companies of interest to the FIU have opened payment accounts abroad with different payment and e-money institutions. As a result, the FIU has made more inquiries to its Lithuanian counterpart than in the past. We also maintain close external communication with Malta, Latvia, the United States, Finland and Germany. In addition, we maintain close and meaningful cooperation with our colleagues in Ukraine, despite their difficult situation.

The Egmont Group, an umbrella organisation of FIUs worldwide, decided to suspend the membership rights of the FIU of the Russian Federation – Rosfinmonitoring – on 18 October 2023. Estonia's position in support of the decision highlighted, among other things, that:

Rosfinmonitoring supports the illegal Russian war machine by acting contrary to what is expected from FIUs;

Despite international anti-money laundering standards prohibiting the financing of weapons of mass destruction, the Russian Federation purchases weapons from North Korea, thereby financing the latter's nuclear programme;

The Russian FIU also maintains a list of 'terrorists and extremists' to which journalists and other persons are often added for mainly political reasons and which is used, among other things, to limit their access to financial and basic payment services as a form of punishment;

Rosfinmonitoring opened branches in the occupied Ukrainian territories, clearly demonstrating support for its country that violates international agreements and human rights.

Rosfinmonitoring and its head are also included in the EU's 12th package of sanctions under the so-called freezing sanction.

From an anti-money laundering perspective, the FIU is primarily involved in strategic cooperation at the global and European levels regarding crypto-assets, virtual asset service providers and technological advancements. The FIU staff have delivered presentations on these topics at conferences and workshops organised by different organisations and national FIUs.

In addition, the FIU participates in the advisory board on data analysis of the EU's Anti-Money Laundering and Countering the Financing of Terrorism Authority (AMLA) to be established. The establishment of the

The creation of AMLA will significantly change the work of the FIU.

AMLA is part of the EU's new anti-money laundering package, which also comprises a new regulation on transfers of funds, a new regulation setting out anti-money laundering requirements for the private sector and a directive on anti-money laundering. The FIUs of EU Member States have been exchanging information and contributing to law-making on these issues, and wider participation is expected in the current year and the next. As the process will significantly change the work of the FIU and its supervisory function, new information on its content and impact will be available in the upcoming yearbooks.

The FIU also made preparations to join the Europol Financial Intelligence Public Private Partnership (EFIPPP) working group. This platform is the first transnational information-sharing platform in the field of combating money laundering and terrorist financing. It provides an environment for cross-border cooperation and information exchange between Europol, competent authorities (including FIUs and law enforcement authorities) and private sector representatives (eg banks).

Disposal restrictions and administrative confiscation

30-day restrictions were imposed in 28 cases in the **total amount of nearly 4.4 million euros,** including in 11 cases of terrorist financing in the total amount of 7,529 euros

60-day restrictions were imposed in 50 cases in the **total amount of nearly 9.5 million euros,** including in 11 cases of terrorist financing in the total amount of 5,779 euros

365-day restrictions were imposed in 35 cases in the **total amount of 3.85 million euros**

10 compliance notices were issued for the transfer of **nearly 1.36 million euros** to state ownership

In the event of suspicion of money laundering or terrorist financing or to stop a criminal activity, the FIU may impose restrictions on the disposal of assets. In doing so, the FIU employs measures to ensure the preservation of assets derived from criminal activity, preventing their further legalisation, or to counter the financing of terrorism. The FIU may also impose disposal restrictions at the request of an FIU of another country.

In 2023, the FIU imposed restrictions on the disposal of assets derived from investment fraud, BEC fraud, smuggling and other criminal activities. Restrictions were mainly imposed on funds in accounts, but also on bonds, cash and crypto-assets.

One-year disposal restrictions, which require the FIU to obtain court authorisation, were imposed in 35 cases for a total amount of 3.85 million euros. This marks a sevenfold increase in the number of restrictions and a 2.5-fold increase in the total amount compared to 2022.

The number of restrictions related to terrorist financing is significant, but the amounts characteristic of terrorist financing are typically smaller. More information about countering the financing of terrorism can be found in the next chapter.

Assets previously restricted by the FIU were seized in 2023 in the total amount of nearly 9.2 million euros. In 2023, the Prosecutor's Office confiscated funds in the total amount of 2.43 million euros, including 1.66 million in relation to money laundering (Prosecutor's Office Yearbook 2023).

On two occasions, at the request of an FIU of another country, restrictions were imposed on the disposal of assets totalling 212,000 euros, which were subsequently seized during criminal proceedings.

ADMINISTRATIVE CONFISCATION

The Money Laundering and Terrorist Financing Prevention Act (MLTFPA) contains a so-called administrative confiscation provision (subsection 7 of § 57 of the MLTFPA). In the event of suspicion of money laundering or terrorist financing, this provision provides the basis for the transfer of assets to state revenue if, during the period of restrictions imposed on the disposal of assets by the FIU, the owner of the assets or the beneficial owner of the assets held on the account cannot be identified.

The purpose and content of administrative confiscation is not to convict or punish a person, but to restore legality by confiscating from a person who is not the beneficial owner of the assets the assets that do not belong to them and by giving the beneficial owner of the assets the opportunity to recover their assets.

We can discuss the limitations regarding the use of the administrative confiscation provision in Estonia in more definitive terms in next year's yearbook. More specifically, 57 new court cases were initiated in 2023 in relation to the restrictions imposed by the FIU, the majority of which are still pending a final resolution. Nonetheless, the FIU has been granted a number of authorisations to transfer assets to state revenue.

[2] Some of the 60-day restrictions are a continuation of the 30-day restrictions that began in 2022 and are not reflected as 30-day restrictions in the 2023 statistics.

ADMINISTRATIVE CONFISCATION AS UNDERSTOOD BY THE FIU IN ACCORDANCE WITH INTERNATIONAL STANDARDS, LAW AND CASE LAW

Different directives and FATF Recommendations do not require the establishment of a legal framework to allow for the confiscation of assets in the absence of a conviction. These types of confiscation are called non-conviction based confiscations in specialised literature, which can be a subtype of criminal procedure or so-called civil or administrative confiscation.

The FATF Recommendations establish the minimum technical framework that a country must have in place. While the FATF Recommendations do not explicitly mention confiscation without conviction, the interpretive note to Recommendation 4 expresses this explicitly together with a reference to consider reversed burden of proof. However, the effectiveness of countries is assessed based on the FATF Methodology. Therefore, a country may be technically compliant with the standards but still not effective. In addition to confiscation during criminal proceedings, the FATF Methodology also considers, for example, the above-mentioned civil and administrative confiscation, ie indicators of when a national confiscation system can be considered effective.

In the MONEYVAL evaluation, Estonia received a score of 2 out of 4 for confiscation, with criticism directed at the country's inadequate performance in confiscating assets during criminal proceedings. An increasing number of countries around the world are using the option of confiscating assets without requiring a conviction.

The Estonian state introduced administrative confiscation to a greater extent in 2017. Although this may not be apparent from relevant explanatory notes or verbatim reports, the aim, at least in oral discussions, was to overcome shortcomings related to confiscation in criminal proceedings, among other things. These shortcomings included, among others, the limited ability to prove underlying criminal activity in each criminal offence, particularly due to constraints on cooperation between investigative authorities (eg countries that do not respond to inquiries, delays in requests for legal aid). At the same time, the Estonian state considered that its primary money laundering risk involves assets derived from criminal activities committed in other countries, which were or are concealed through the Estonian monetary and financial system, ie Estonia is used as a transit country for money laundering. It is precisely for such cases, aiming to prevent the exploitation of the Estonian monetary and financial system and thereby mitigate potential reputational risks, that the institute of administrative confiscation was established in 2017, with extended rights for the FIU.

If in the case of conviction for money laundering, all the necessary elements of a criminal offence must be shown, including both objective and subjective elements, the grounds for confiscation are different in the case of administrative confiscation. For administrative confiscation:

- there must be suspicion that the restricted assets are associated with money laundering or terrorist financing;
- the restriction must be necessary for ensuring the preservation of assets;
- the possessor or owner of the assets suspected of being associated with money laundering must have failed to prove the legal origin of the assets to the FIU;
- the possessor or owner of the assets suspected of being associated with terrorist financing must have failed to eliminate the suspicion that the assets are being used for terrorist financing;
- it must be demonstrated that the FIU has also failed to identify the owner of the assets or the beneficial owner of the assets held on the account.

So far, the use of the institute of administrative confiscation has been rather modest. In 2022, the FIU's analysis revealed several dozen cases where the initiation of criminal proceedings was not possible or appropriate for different reasons. At the same time, suspicions of money laundering remained with regard to the restricted assets.

These cases primarily fall into three specific types.

The first group of cases concerns the laundering of banknotes brought to the Bank of Estonia, suspected by the FIU of having been stolen from the Central Bank of Libya. In 2023, two cases resulting in the transfer of assets to state revenue reached a final decision. To prevent assets derived from criminal activity from entering the legal financial system, the exchange of these banknotes should also be refused elsewhere, similar to the practice in Estonia, or other available means under national law should be used.

CASH EXCHANGE ATTEMPT RESULTING IN CONFISCATION

In the summer of 2022, two persons visited the museum shop of the Bank of Estonia to exchange damaged banknotes. Upon assessing the damage to the banknotes, it became evident that they exhibited characteristics consistent with a certain criminal offence.

A UN report issued in September 2018 detailed that during the Libyan civil war in late 2017, approximately 160 million euros, 2 million dollars and 640 Libyan dinars in cash and silver were taken from the central bank's branch in Benghazi to an unknown location. The banknotes had (waste)water damage.

Given that there had likely been an attempt to clean the banknotes afterward, their condition had deteriorated even further. According to public sources, the banknotes taken from the central bank's branch that were in good condition were used to buy equipment and weapons. However, it is estimated that half of the banknotes were so badly damaged that they were sold for less than their face value to the so-called Turkish mafia.

Since late 2018, damaged, high-denomination euros have started to circulate in Europe that may originate from the assets embezzled from the branch of the Libyan central bank.

When assets exhibiting damage typical of so-called Libyan money caught the attention of the FIU, their disposal was restricted. Since it was ultimately not possible to identify the beneficial owner of these assets, they were confiscated from the persons and, based on the authorisations granted by the administrative court in 2023, a total of 9,000 euros worth of assets were transferred to state revenue. Other similar applications have been prepared. However, the persons wishing to exchange banknotes in new cases have been different natural persons.

The owner of the assets has the right to recover the amount transferred to state revenue within three years of the date on which the assets were transferred to state revenue.

The second case, according to the suspicion of the FIU, involves cash stolen from Ukraine that, for example, 15 different persons attempted to transport across the Russian-Estonian border within a single day, all carrying round sums of cash, mostly in the amount of 350,000 hryvnia. The only difference among them was the origin story of the banknotes.

In the third case, the FIU determined that the accounts of natural persons had received funds which raised reasonable suspicion that they were derived from criminal activity. The FIU discovered that the 'path' of the funds involved approximately 15 transactions which, in one example, passed through several banks in Estonia and three other countries, and two foreign and three Estonian companies controlled by the same persons were used. The transfers of funds exhibited several characteristics specific to money laundering, also known as typologies.

We will be able to present the final solutions of the last two cases in next year's yearbook.

With the authorisation of the court, the FIU issued a compliance notice for the transfer of assets to state ownership on ten occasions, for the total amount of nearly 1.36 million euros. With the authorisation of the court, crypto-assets, which had previously been subject to disposal restrictions by the FIU in 2022 based on court authorisation, are now being transferred to state revenue for the first time.

On the basis of the compliance notices issued in 2023, a total of 104,562 euros were transferred to state revenue. The remaining part is delayed because the assets in the form of virtual assets are in the possession of a foreign person in connection with the merger of the company with another company.

TWO CASES OF CRYPTO-CURRENCY BEING TRANSFERRED TO STATE REVENUE

In one case, assets suspected of deriving from investment fraud were found to have been transferred to an account opened with a virtual asset service provider authorised in Estonia on the basis of forged documents. No other links with Estonia were identified. In the course of the procedure, neither the victims nor the offenders could be identified.

In the second case, it was discovered that a person suspected of committing fraud in a foreign country held an account with an Estonian virtual asset service provider and there was reasonable suspicion that the assets in the account were derived from criminal activity. The assets were transferred to state ownership because the person failed to prove the legal origin of the assets and the owners and beneficial owners of the assets could not be identified.

Reporting

12 500

reports submitted over the year

including approximately

10 000

suspicious transaction or unusual transaction reports

of which more than

4000

were reports concerning fraud

The reports submitted by market participants are valuable sources of information for detecting and preventing criminal offences. Selected reports undergo in-depth analysis and, based on the reports, disclosures are made to investigative authorities or disposal restrictions are imposed. The information contained in the reports is also used in the tactical and strategic analysis of the FIU.

Among the obliged sectors, credit institutions are the most risk-aware and submit the most substantive reports. The quality of submitted reports varies across banks in terms of both form and content, but they reflect progress in the implementation of due diligence measures.

In all other sectors, the main issue is the low level of reporting activity. There are only a few active reporting entities among financial institutions, traders and professionals (excluding notaries) who submit more than ten reports per year.

The main issue is the low level of reporting activity

In terms of report types, there was a positive increase in the number of suspicious transaction reports (STRs) in the sector of gambling operators and financial institutions, indicating improved detection of suspicious money laundering activities. Several sectors saw an increase in both the number of terrorist financing reports (TFRs) and the number of persons submitting these reports. It is evident from the received TFRs that market participants are also better able to identify and analyse these cases compared to the past. A more detailed statistical overview by sector and types of report can be found in the '2023 in numbers' section at the end of the yearbook.

Please note:

The report must be submitted immediately, but no later than two working days after the detection or suspicion of the activity or circumstances.

Reporting of cash transactions exceeding 32,000 euros cannot be urgent. The reporting entity must establish suspicion through the implementation of due diligence measures.

The typology notices of the FIU offer guidance on how to recognise risks using the described indicators and be more proactive in identifying potential new criminal patterns.

To enhance the quality of reporting in the future and streamline the process for both the FIU and market participants, the FIU has initiated the development of a customer portal.

BEST REPORT OF THE YEAR

The best report of the year once again came from a bank.
Strengths of the report:

- **The transactions were analysed substantially**
- **The information gathered during the implementation of due diligence measures was analysed in great detail**
- **The report was logically structured**
- **The suspicions were clearly presented**
- **The report was submitted promptly**
- **The form of the report was correct**

The story behind the report

The credit institution became suspicious of the transactions made on the account of an Estonian company. The transactions took place between the accounts of several related companies and it was suspected that the transactions were fictitious. Both the ostensible nature of the transactions and their pattern were indicative of benefit fraud and tax fraud.

The analysis conducted by the credit institution revealed that the Estonian companies involved in the chain of transactions were related to each other through economic activity and that the board members of the companies had a blood relationship.

The bank implemented due diligence measures, on the basis of which it asked the customer to provide the source documents of the transaction. The invoices and other documents provided by the customer indicated that the transactions in the account involved the purchase and sale of used agricultural machinery and other agricultural goods.

The credit institution analysed very carefully and thoroughly the market prices of the exchanged goods and equipment and whether the ownership of the equipment changed.

The analysis revealed that the selling price of the equipment was several times above market value. Both the selling price of the equipment and the movement of money on the basis of the invoice indicate the ostensibility of the transaction. In addition, according to the Transport Administration, the ownership of the equipment had not changed, which also indicates the ostensibility of the sale.

The credit institution also noted a significant gap of over a year between the invoices submitted by the customer and the corresponding payments, further suggesting the ostensible nature of the transactions.

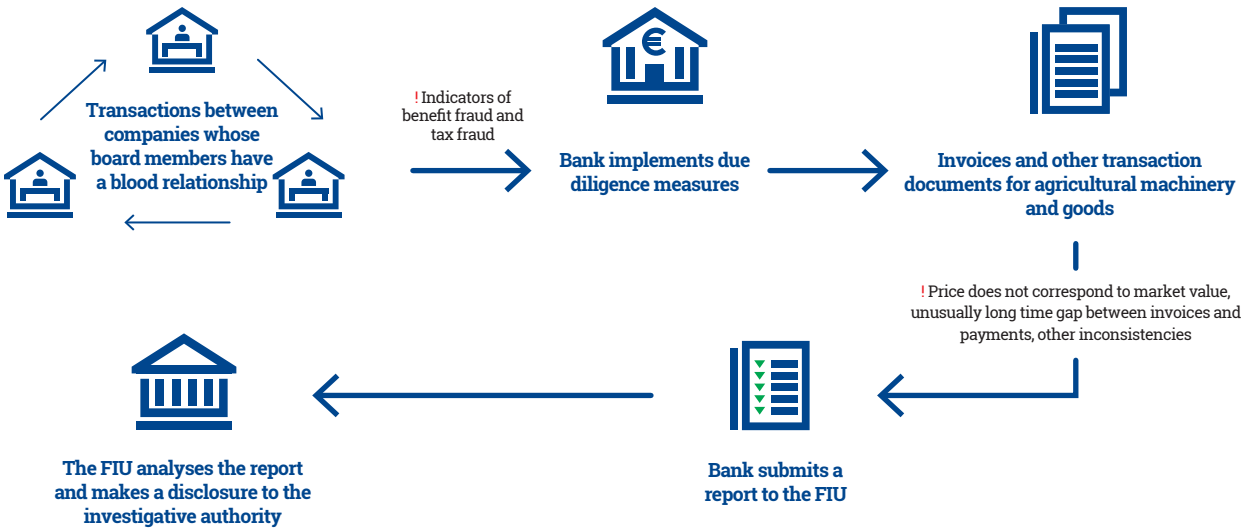
By analysing the account statements of other counterparties of the customer (companies that are customers of the same credit institution), the credit institution came to the conclusion that the same funds were repeatedly transferred between the same companies within a short timeframe. Such money transfers are unusual and not typical of regular economic activity.

Taking into consideration the fact that there were indications of ostensibility in the purchase and sale transactions, which is also supported by the unusual movement of money between the same companies, suspicion arose that the described transactions did not actually occur on such a scale.

Consequently, there are grounds for suspecting that the transactions described above were carried out for the purposes of benefit fraud and tax fraud.

The credit institution submitted a report to the FIU, referring to the typology notice on trade-based money laundering published by the FIU.

The FIU further analysed the report and subsequently made a disclosure to the investigative authority based on the report.



Countering terrorist financing

There are two main differences between terrorist financing and money laundering:

1. **In addition to criminal activity, funds can also originate from legitimate sources,** such as income, grants and donations, membership fees, sales, organising events and rental income.

2. **Money is a means, not an end.** The purpose is to use the funds to carry out or facilitate terrorist activities (including recruitment, ideology dissemination, training, subsistence, travelling, and purchase of even the simplest of weapons). Thus the amounts involved may be very small, but it is the ideological aspect that is important.

Risk profile

TERRORIST FINANCING RISK LEVEL IN ESTONIA IN 2023: MEDIUM

[3] In addition to the three primary stages of terrorist financing, the process may also encompass: **storing**, ie the holding of funds to keep them safe and potentially increase their value; **obscuring**, ie obscuring the origin, ownership, destination, etc of funds to conceal their actual purpose; **managing**, ie the planning and organisation of funds, the involvement of relevant structural units or other parties (eg accountants, investors), where necessary.

The distant Israel-Hamas war also significantly affects the risk profile of terrorist financing in Estonia. Firstly, it brought about a rapid collection of donations and grants for the protection of civilians in the conflict zone – in a situation where the final use of the funds could not be ascertained. This also involved attempts to transfer funds to organisations operating in Gaza and the West Bank, including Hamas-involved parties. The conflict will continue to significantly impact the risk environment of terrorist financing also in 2024.

Furthermore, the conflict has undoubtedly contributed to an increase in the vigilance and awareness of market participants in Estonia, which in the long run can have a positive effect on the prevention of terrorist financing among Estonian market participants. In the Middle East, however, the reaction of the West – Europe in particular – to the Israel-Hamas war has caused major disappointment, which is why we are likely to see a wave of radicalisation in the long term. In any case, this will result in increased transfer and collection of funds, including for terrorist purposes.

Hamas' main sources of income for raising funds have been:

- **Support of Iran**
- **Taxation** (control over the territory, border crossing points and the local population)
- **Exploitation of charitable organisations**
- **Crowdfunding campaigns**
- **Investing and shelf companies**

Short study 'Financing models of the terrorist organisation Hamas'
The Estonian Financial Intelligence Unit, 2023

In terms of terrorist financing, the risk environment of Estonia is significantly influenced by the virtual asset service provider sector. Just like ordinary people, radicalised individuals and terrorist organisations are increasingly using virtual assets, combining them, for example, with crowdfunding platforms and traditional hawala[4] principles. To this end, we have conducted targeted outreach to raise the sector's risk awareness and capacity.

We are also seeing the fruits of our labour – increased risk awareness and enhanced capacity – in one of the most important cases of the year. Thanks to the actions taken by a market participant, the FIU, in cooperation with the Estonian Internal Security Service, was able to identify a network of terrorist financiers. The case showed the materialisation of risks associated with virtual assets on a large scale. Specifically, we identified an 18-member network intending to conduct crypto-currency transactions through an Estonian service provider.

The risk profile of Estonia is also influenced by its open economic environment, which allows for the relatively easy establishment of companies, thanks – amongst others – to the e-residency programme. In this respect, it is important to keep in mind countries with a higher risk of terrorist financing[5]. The role of company service providers in recognising signs of terrorist financing is crucial. Greater attention and support are also needed for higher-risk non-profit associations, in the case of which vulnerabilities can encompass cross-border transactions, partners in conflict areas and lack of control over the final use of funds.

The risk profile of the coming years will be shaped by the global nature of terrorism: ideologies spread and inspiration is obtained, among other things, from the online environment, transcending national borders. Both in Europe and beyond, it is increasingly seen that different types of reactionary ideologies reinforce each other. Despite their apparent differences, extremist ideologies increasingly share common denominators, both in terms of enemies and strategies. This is increasingly evident in the terrorist financing challenges we face.

While Islamic extremism is increasingly recognised, general awareness of other forms of extremism is still low. On one hand, the ideologies of these groups seeking a violent change of power are gaining traction; on the other, some countries have initiated national bans against them. These include, among others, violent far-right extremism, the financing of which is much more challenging to address compared to Islamic extremism. Additionally, one of the challenges is that organisations supporting violent far-right or -left extremism are not included in the UN or EU sanctions lists.

[4] ***Hawala*** is a trust-based traditional method of money transfer that is common in the Middle East, Africa and Asia, where money does not need to be physically sent to its destination. For instance, movable or immovable property may be accepted instead of cash in a destination country with a community-based settlement system.
[5] A list of countries with a higher risk of terrorist financing (so-called risk countries) can be found on the website of the FIU: **www.fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh**

USE OF CRYPTO-CURRENCY TO SUPPORT A TERRORIST ORGANISATION

Supported terrorist organisation: Palestinian Islamic Jihad
Crypto-currency: Tether (USDT)
Amount frozen: 8 963 USDT (u 8 205 EUR)
Related parties: 18
Cooperation: Estonian Internal Security Service, virtual asset service provider, foreign FIUs

Thanks to the vigilance of a market participant, we identified a (predominantly) Gaza-based network that had conducted transactions in virtual assets on other platforms using different crypto addresses associated with the terrorist organisation Palestinian Islamic Jihad.

The funds were not only transferred to the terrorist organisation but also received from it, indicating direct action in the interests of the organisation. The amounts moved by the network were significant in terms of terrorist financing, reaching hundreds of thousands.

Members of the network then attempted to conduct transactions through an Estonian market participant by depositing funds here.

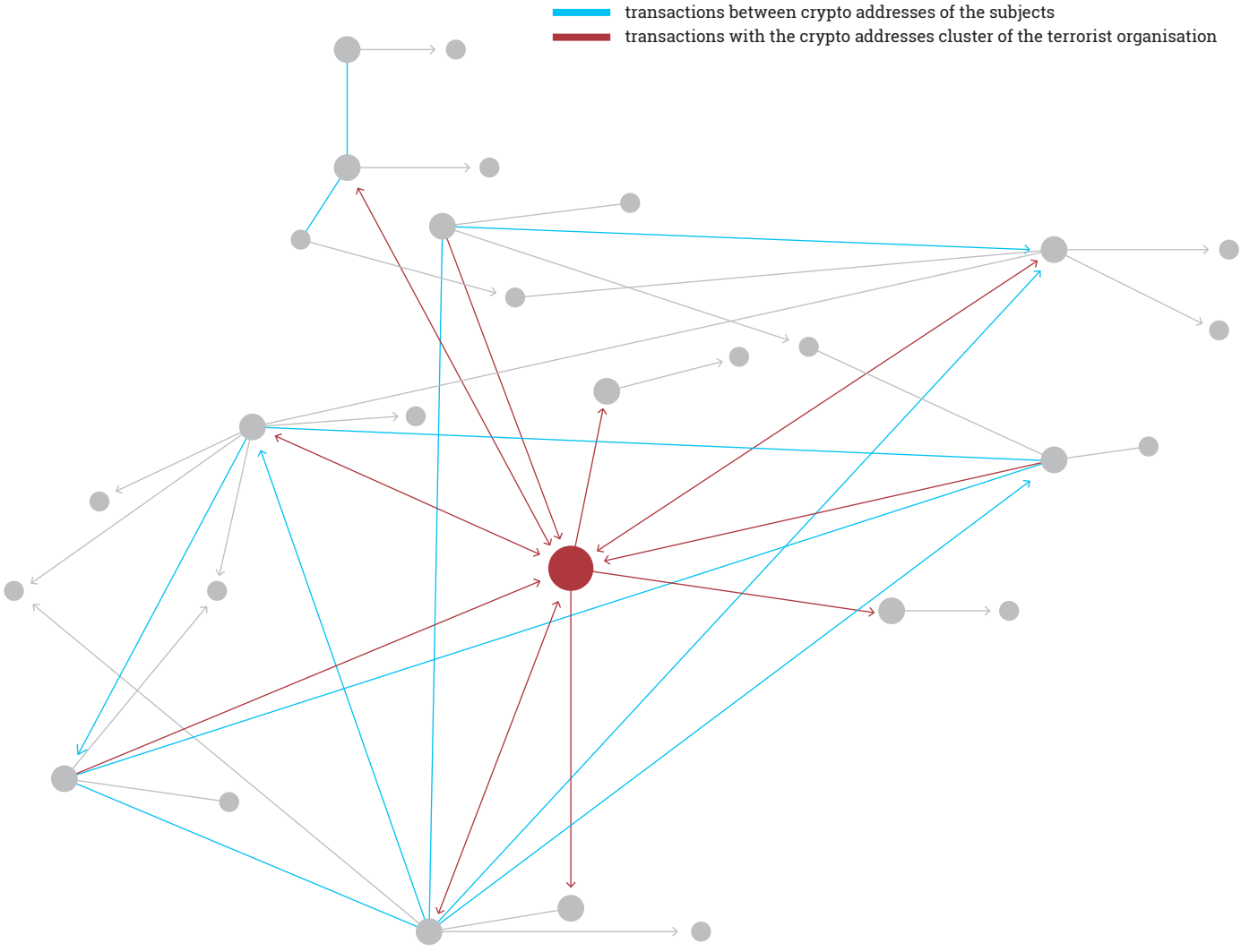
For an authorised virtual asset service provider in Estonia, this represented a fairly standard business model for the sector: a correspondent relationship, which in turn poses a higher risk. This means that the Estonian virtual asset service provider had a legal person customer situated in another jurisdiction, which in turn had natural person customers in a conflict zone (so-called end customers). The service provider authorised to operate in Estonia faced apparent challenges in obtaining full information from the customer about its end customers. However, eventually, due to the seriousness of the case, this information was successfully obtained.

The FIU issued compliance notices to the market participant for the submission of additional information and imposed restrictions on the transactions.

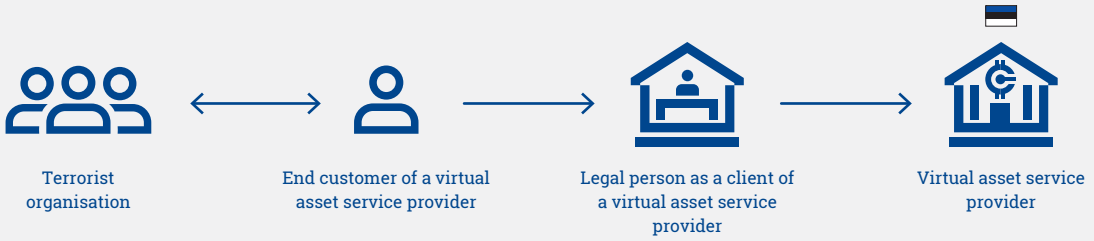
In the end, we used sanctions as a tool to prevent terrorist financing. As the EU[6] has designated Palestinian Islamic Jihad as one of the organisations subject to the freezing of funds, other financial assets and economic resources, the assets of the network that were located in Estonian jurisdiction were frozen. The total amount frozen was 8,963 USDT (crypto-currency Tether), ie approximately 8,205 euros.

6 Annex to Council Regulation (EC) No 2580/2001 of 27 December 2001

DETECTED TRANSACTIONS BETWEEN CRYPTO ADDRESSES



ANATOMY OF A TRANSACTION



Palestinian Islamic Jihad is the second largest terrorist organisation in Palestinian territories after Hamas. However, it is a small clandestine movement that, unlike Hamas, does not provide social services or participate in the work of power structures. Its members also originated from the Egyptian Muslim Brotherhood, which was not radical enough for them. Despite being Sunni, they drew inspiration from the 1979 Iranian Islamic Revolution, which established a theocratic regime. Although, on the one hand, the organisation cooperates with Hamas, on the other, they are rivals, with differences in their tactical, strategic and ideological approaches. The main financial supporter of the organisation is Iran. Main area of operation: Gaza, West Bank. Including also Lebanon, Syria and Iran.

THE HUMANITARIAN AID CASE

The FIU received reports where donors wished to send money to private persons and organisations in the Gaza Strip for humanitarian purposes through an Estonian credit institution.

Among the organisations, the Hamas-linked Gaza Now was identified.

The credit institutions stopped all the upcoming transactions that they noticed.

The FIU published a typology paper / short study to draw the attention of market participants and the public to the financing models of terrorist organisations associated with the Israel-Hamas war, highlighting specific risk indicators.

Given the sensitive context of humanitarian aid, it is important to ensure that donations are made through official and secure channels to well-established and reputable organisations after having checked their background. The FIU advises against donating to persons with whom you have no personal connection, especially if you found their information on social media.

Terrorist financing reports

273
suspected terrorist financing reports

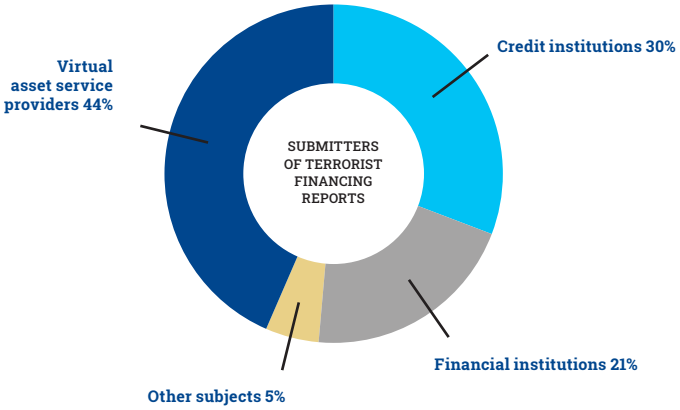
40
reports less compared to 2022

95%
of reports were submitted by three sectors in total

Based on the terrorist financing reports submitted to the FIU last year, it is evident that market participants' awareness of terrorist financing is on the rise. Reporting entities are increasingly seeking and incorporating relevant information from open data sources and are able to identify potential links with terrorist organisations and conflict zones.

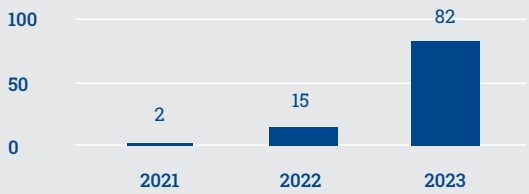
The total number of reports is slightly lower than in the past, but the content and quality of the reports are improving. However, sectors that do not submit any reports (gambling operators, providers of trust and company services, non-profit associations), those that submit reports of insufficient quality (notaries) or those that submit too few reports given the size and volume of the sector (virtual asset service providers) remain areas of concern.

Nearly one-fifth of the highest-risk sector, virtual asset service providers, submitted terrorist financing reports, which is a significant improvement compared to previous years. The circle of reporting entities has expanded and the quality of the reports has improved. This improvement can be attributed to raising awareness among virtual asset service providers, more effective implementation of due diligence measures and more skilful use of analytical tools. On the other hand, the fact that only 20% of service providers submitted reports may indicate that the remaining 80% lack adequate business commercial relationship monitoring solutions to identify circumstances indicative of terrorist financing.



A significant shift in countering terrorist financing can be seen in the work of credit institutions. In particular, the reporting activity of banks has increased dramatically compared to just a few years ago.

Number of TFRs from banks



During the year, the FIU received a significant number of terrorist financing reports involving persons who do not reside in Estonia but use Estonian market participants for their transactions. This shows that, like terrorism, the fight against terrorist financing is international by nature and Estonian market participants can also gather necessary information about radicalised individuals operating in third countries. By informing the FIU of suspected terrorist financing activity, this information will also reach the country that needs it the most.

In relation to terrorist financing or suspicion thereof,

- 30-day restrictions were imposed 11 times in the total amount of 7,529 euros
- 60-day restrictions were imposed 11 times in the total amount of 5,779 euros
- freezing of funds was imposed 18 times in the total amount of 8,205 euros

Cooperation in preventing terrorist financing

While the resolution of terrorist financing cases relies heavily on close cooperation with foreign FIUs, the active participation of the FIU in international cooperation projects also contributes significantly to building a broader knowledge base.

A joint report of the Egmont Group on the use of virtual assets for terrorist financing, coauthored by analysts from the Estonian FIU, was published.

The Counter Terrorist Financing Taskforce – Israel (CTFTI), led by the FIUs of the Netherlands, Israel, Germany and the United States of America, primarily targeted the prevention of terrorist financing of two terrorist organisations: Hamas and Palestinian Islamic Jihad.

The United Nations Office on Drugs and Crime (UNODC) working group discusses current terrorism cases in different jurisdictions, the activities of extremist groups (primarily violent far-right and Islamic extremism) and the associated challenges.

In 2023, in addition to the completed MONEYVAL evaluation, Estonia also underwent a UN evaluation visit which focused on Estonia's counter-terrorism practices and provided recommendations for overcoming development gaps. On the one hand, in terms of terrorist financing, the evaluation reports offered valuable recommendations for reviewing internal processes. The FIU has already started to implement these recommendations. On the other hand, the recommendations were tied to specific steps aimed at enhancing nationwide cooperation.

FIU intends to identify the targets of terrorist financing in a more proactive and risk-based manner

These proposals can be implemented in cooperation with competent authorities and the private and public sectors.

Based on the recommendations of MONEYVAL and the UN evaluation report, the FIU intends to identify the targets of terrorist financing in a more proactive and risk-based manner. This will entail, among other things, a greater contribution to strategic analysis in this area, the development of sector-specific guidelines for higher-risk sectors and a proactive approach to awareness raising. The latter involves both training and information sessions, studies and typology papers, as well as different forms of cooperation. More active information exchange between competent authorities and credit institutions is a positive step toward strengthening cooperation with market participants. Alongside this, engaging in dialogue with virtual asset service providers and non-governmental organisations is also important.

International Financial Sanctions

IN 2023, A TOTAL OF 606 INTERNATIONAL SANCTIONS REPORTS WERE SUBMITTED

Under financial sanctions:

59
authorisations for a derogation were granted

As of 31.12.2023, a total of

33
million euros were frozen

59 338
euros in assets were not made available

A deposit restriction totalling

197 530
euros was applied[7]

The key themes of the year included sanctions circumvention and situations where several types of sanctions were intertwined, such as trade restrictions, eg ban on goods or services and financial sanctions combined.

International sanctions reports (ISR) submitted to the FIU show that obliged entities have begun to pay more attention to analysing how sanctions are circumvented. The increase in the number of reports referring to this compared to 2022 is almost six-fold, accounting for 43% of the total number of ISRs submitted.

Primarily, the FIU is informed about situations in which Estonian companies continue to cooperate with Russian business partners with whom business was conducted before the start of the Ukrainian war through intermediaries. For this purpose, companies with an opaque background registered in third countries are actively used. This may be a company that has been operating for a long time, but also a legal person registered immediately after the war, to which, for example, goods included in the sanctions list are sold and through which funds are transferred to Estonia.

As the number of payments between Russia and Estonia has dropped significantly, the main risks of violating financial sanctions are associated with situations in which it is not funds (eg money) but rather economic resources (eg goods) that are made available to the subject of the financial sanctions. The link between

The main risk of violating financial sanctions is related to economic resources being made available to designated persons.

the application of financial sanctions and the trade restrictions is particularly important here. Namely, companies registered in third countries are indicated as recipients of goods the transfer of which to Russia is prohibited. In reality, however, goods may be re-exported to Russia from a third country. The link with financial sanctions arises when the recipient or the manufacturer of the goods is the subject of financial sanctions. The recipient of the goods may also be subject to sanctions through its beneficial owner. This means that goods being transported to Russia, thereby concealing the end user of the goods, may not only violate the restriction on goods, but also make resources available to the designated person subject to asset freeze, thereby violating the financial sanctions.

[7] **Were frozen –** preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, value, location, ownership, possession, character, destination or other change that would enable the funds to be used, including portfolio management. **Were not made available** – a transaction or action was refused because it would have resulted in making funds available to a person subjected to financial sanctions, or violation of a financial sanction. **A deposit restriction was applied** – funds not allowed into an account by credit institutions, as the total value of a person's deposits per credit institution may not exceed 100,000 euros.

VIOLATION OF FINANCIAL SANCTIONS AND TRADE RESTRICTIONS

Information about companies that up until the end of 2021 were actively engaged in the intermediation of fine electronics to Russia was provided to the Financial Intelligence Unit.

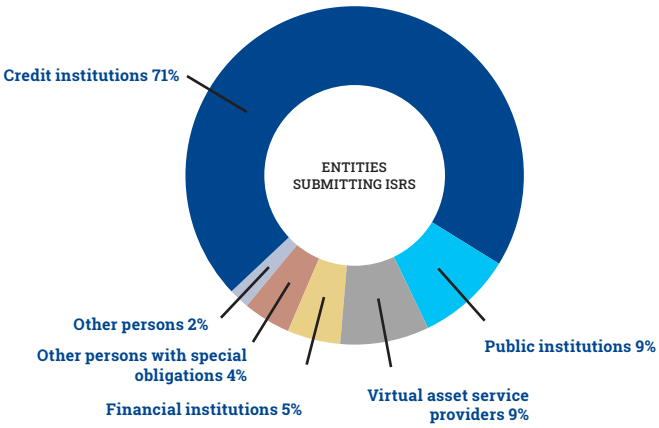
The Financial Intelligence Unit found that after the ban came into force, an Estonian company started selling electronics produced in the West to companies in Turkey and Kazakhstan. The goods did not pass through Estonia.

In the course of its investigation, the Financial Intelligence Unit found that the transaction partners of third-country companies are located in Russia and are related to persons included in the European Union sanctions lists.

With the re-export of goods to Russia, both the trade restrictions and the financial sanctions were violated, as economic resources were made available to entities included in the European Union sanctions lists.

REPORTING

Credit institutions submit the most reports, but more and more public authorities are asking the FIU for feedback on their analysis conducted on the potential links to a designated person. In the case of credit institutions, it can also be seen that the reports have become more substantial. This means that there is a general ability to analyse the ownership and control criterion and, based on this, to draw conclusions as to whether the restrictions imposed on individuals extend to related business entities.



VIOLATION OF FINANCIAL SANCTIONS BY SALE OF GOODS

Based on a bank's report, the Financial Intelligence Unit established that an Estonian company had sold goods to Russian companies related to persons included in the European Union sanctions lists.

The company failed to identify the owners/beneficiaries of its business partners and financial sanctions were violated by making economic resources available.

Although the supply of goods to Russia was not prohibited, it constituted a violation of the financial sanctions, since economic resources were made available to the designated person through the transaction.

THE AMOUNT OF FROZEN ASSETS INCREASED

The amount of frozen assets in Estonian credit institutions and the Tax and Customs Board increased during the year. While in the first quarter of 2023, there were just over 18 million euros in frozen assets, by the end of 2023 the total amount of frozen assets is slightly more than 33 million euros. The main change in frozen assets occurred at the end of the first quarter, when payments were received to the company accounts in Estonian credit institutions from assets (mainly fertilisers) sold under a derogation allowed for in the regulation. The subject of the derogation was the goods belonging to a designated person subject to financial sanctions and the payments for those goods were allowed under the previously concluded agreements clause. Changes in the volume of frozen assets are also due to covering the costs necessary for managing company assets, eg utility payments. Such payments are allowed only if the FIU has issued a relevant permit.

REFUSAL TO GRANT AN AUTHORISATION FOR A DEROGATION FROM FINANCIAL SANCTIONS

The EU regulations allow for derogations from the restrictive measures imposed. These derogations include the release of certain frozen assets including funds and economic resources if they are deemed necessary, for example in transactions involving agricultural and food products addressing the food security in third countries.

A company owned by a designated person operating in Estonia submitted an application to the FIU in order to get an authorisation for the derogation described above for the provision of logistics services to the fertiliser producers operating in Russia with the intention to sell their fertilisers under this derogation.

The FIU had so far not granted authorisation for any fertiliser sales transaction that would have involved bringing fertiliser produced by a company of a designated person into the territory of Estonia. In essence, the request basically sought a general authorisation for future transactions of an indefinite number and content. Such an authorisation would have involved the use of Estonian territory for the transport of the goods of the designated person.

This derogation set out in the EU Regulation allows the competent authority to authorise such transactions based on specific and case-by-case assessment only, to ensure, inter alia, that each transaction is directly necessary to address the food crisis.

The conditions for granting the derogation sought by the applicant were therefore not met, as a general authorisation was sought for unspecified future transactions.

The FIU refused to grant authorisation for said derogation.

LESSONS FROM THE FERTILISER CASE

The 2022 Yearbook of the FIU thoroughly covered the so-called fertiliser case. In 2022, the beneficial owners of two Estonian companies – AS DBT and EuroChem Terminal Sillamäe OÜ – were added to the EU sanctions list, as a result of which the assets of both companies were frozen, including hazardous chemicals in their terminals. However, a few months later, the Consumer Protection and Technical Regulatory Authority made a compliance notice according to which both companies had to sell and/or dispose of hazardous chemicals in cooperation with the owners of the goods. In 2023, the Financial Intelligence Unit granted financial sanction derogation authorisations for the release and sale of these chemicals under the regulation of the EU Council and the Authority's compliance notice. These authorisations constituted the vast majority of all the authorisations granted for derogations.

i

AS DBT has two Category A major hazard establishments, one of which is located in the Muuga port (terminal for the storage of fertilisers in bulk, including ammonium nitrate) and the other in the port of Sillamäe (terminal for storage of liquefied ammonia and liquid fertilisers).

EuroChem Terminal Sillamäe OÜ has two Category A major hazard establishments in the port of Sillamäe (terminals for storage of liquefied ammonia, liquid fertilisers and liquid flammable chemicals). In addition, EuroChem Terminal Sillamäe OÜ stores bulk goods (fertilisers, feed additives).

The Financial Intelligence Unit has granted derogations for the sale of fertilisers **for nearly 117 million euros.**

Almost 54 million euros of this amount has been received or is being received by Estonian credit institutions and will be frozen

The remaining **nearly 63 million euros** received from the sale of fertiliser have been frozen in other EU Member States with which the Financial Intelligence Unit has

The fertiliser case is a very telling example of how the obligation to apply financial sanctions is complex and that the challenges are not only for the subject of sanctions but also for the state that is applying sanctions. While the freezing of funds is generally not an unreasonably burdensome task for a credit institution or other entities, compliance with the obligation to freeze economic resources, including perishable and depreciable economic resources, may entail both a significant financial cost, irrespective of the relationship of the holder of a particular economic resources to that economic resources or the subject of sanctions, as well as a challenge depending on the specific asset. Such cases clearly show that a sanction can be inconvenient and with effects both for the person against whom it is implemented and for the implementers themselves.

The fertiliser case looks relatively black and white when viewed from afar. Had the hazardous chemicals not been sold, they could have become hazardous to the surrounding environment and humans. The EU Regulation also provides for the possibility that a Member State may derogate from the sanction and allow the unfreezing of economic resources in the interests of the environment and human health, thus providing a legal basis for granting authorisations for the release of fertilisers by the FIU. **However, it should be noted that:**

- **the application of any derogation from sanctions means that the objectives for which the sanctions were imposed are thereby more difficult to achieve;**
- **a derogation must be applied narrowly and not to every need, but only to basic needs;**
- **the application of a derogation must come directly from the need which the derogation regulation is designed for;**
- **a derogation can be granted only in the presence of the conditions laid down by the entity who imposed sanctions;**
- **by authorising the sale of frozen economic resources (in particular to third countries) further opportunities for the circumvention of sanctions must not be created;**
- **granting a derogation from financial sanctions must not, as a general rule, entail making funds available to the designated person without their immediate freezing.**

Making sure of all this is the task of the FIU, and must be completed within a limited period of time before granting authorisation for a derogation.

The fertiliser case also made clear how, by imposing sanctions, Member States have knowingly taken the risk that the restrictive measures result in higher costs and inconveniences to be suffered not only by designated persons, but also by third persons not subject to restrictions operating in a Member State. This is both in the form of immediate costs, which may arise, for example, from the obligation to preserve frozen assets, and in the form of revenue forgone from commercial activities. All this is tolerated in the hope that the other side will be affected by the sanctions more painfully. Just as Estonians hope that all other EU countries (as well as several other countries implementing similar sanctions) have set as their primary objective to achieve the greatest possible impact of sanctions on its target, rather than finding a more favourable and convenient solution for themselves, it is the responsibility of the Estonian state as well as each natural and legal person of Estonia to comply with the established sanctions and see that they are carried out in accordance with the purpose and the meaning of regulations.

Cooperation in the implementation of sanctions and ensuring their legality

41

information disseminations about circumvention of sanctions to investigative authorities

179

responses to inquiries

10

financial sanctions training and information courses for nearly 2,000 participants

During the year, three anti-Russian sanctions packages were adopted, in which the Financial Intelligence Unit made several proposals through the Ministry of Foreign Affairs that ended up in EU legislation. With regard to financial sanctions, the sanctions packages adopted last year expanded, in particular, the circle of persons subject to an asset freeze.

Also noteworthy was the inclusion of several major Russian banks and the head of the Russian Financial Intelligence Unit (Rosfinmonitoring) on the sanctions list.

RETURN OF LOAN TO A BANK INCLUDED IN THE SANCTIONS LIST

After Estonian credit institutions largely stopped payments to Russia, individuals began to initiate payments from their accounts with an Estonian credit institution to a payment service provider registered in Cyprus.

The FIU found that the money would be transferred from there to a Russian bank or an Austrian bank, and from there to a Russian bank on the EU sanctions list to which loan repayments would be made.

With these payments, funds were made available to a legal person included in the sanctions list (a bank operating in Russia).

Sanctions do not work in isolation and, consequently, international cooperation is important. In order to enforce financial sanctions, the FIU has worked with a number of countries belonging to the sanctions coalition: it has shared information with foreign partners, prepared guidelines for market participants, carried out joint analyses and contributed to the training of third countries. Cooperation between the three Baltic states has been particularly close and effective. All those activities largely directed outside Estonia were crucial in the fight against circumvention and will continue in the future.

The EU financial sanction is applied to a total of nearly 2,000 individuals and entities in relation to activities that undermine or threaten the territorial integrity, sovereignty and independence of Ukraine.

Almost 50 countries have imposed sanctions, including financial sanctions, on Russia, which also broadens their scope.

It is estimated that after Russia's full-scale aggression in Ukraine, the so-called sanctions coalition has imposed sanctions against more than 16,000 individuals and entities.

In national cooperation, the FIU last year made disseminations to an investigative authority on 41 cases of potential violation of sanctions. In most cases, these were spontaneous information disseminations and reports on possible criminal offences, and in some cases the information disseminated by the FIU was added to the case file of an ongoing criminal case. Based on the FIU's disseminations, two criminal proceedings were initiated.

The FIU shared information with supervisory authorities on three occasions. Furthermore, FIU has also replied to inquiries from investigative and supervisory authorities. Additionally, the FIU has assisted investigative authorities in identifying assets related to financial sanction violations located in foreign countries.

In addition to submitting disseminations to the investigative authorities or providing information, the FIU has the following in its arsenal to ensure the implementation of financial sanctions:

- initiating supervision and misdemeanour proceedings;
- issue compliance notices to suspend transactions;
- give feedback as regards to financial sanctions;
- competence to grant authorisations on the basis of a derogation. By setting the conditions for derogation authorisations and supervising the use of such authorisations, the FIU ensures that assets frozen in Estonia are used only as intended and to the extent necessary.

To clarify a financial sanction and draw the attention of market participants to the most important aspects, the FIU has:

- organised or participated in organising 10 private and public sector financial sanctions information and training courses with a total of more than 2,000 participants;
- responded to 179 inquiries;
- notified the market on two occasions by means of letters of notification of the new obligations and measures;
- published an advisory guide for economic operators, typology reports and a study on the circumvention of sanctions using virtual currencies.

Activities for further awareness-rising will continue in the coming years.

The period of adaptation is over

Certainly, the 12th package of sanctions adopted at the end of 2023 is not the endpoint, and further sanctions against Russia must continue to be imposed, implemented and applied. The pace of the adoption of new packages slowed down last year, but it is all the more important to focus on the implementation of the measures adopted and the fight against circumvention. Sufficient time has passed since the beginning of the Russian war against Ukraine for market participants to have the necessary human resources and technological means to identify and prevent violations of financial sanctions and to apply the financial sanction lawfully and promptly.

This means that the actual implementation of the financial sanction, the detection of circumvention and the functioning and aptness of the systems will also be one of the FIU's focus points in 2024. Among other things, this means that the FIU is prepared to react more forcefully to deficiencies identified during supervision and to initiate misdemeanour proceedings within the framework of its competence in a situation where a market participant has breached due diligence or reporting obligations.

The FIU is prepared to initiate misdemeanour proceedings more vigorously in situations where due diligence or reporting obligations have been violated.

The amendments to the International Sanctions Act currently pending in the Riigikogu take into account, in particular, the experience gained over the past two years and the recommendations made in the framework of MONEYVAL and UN evaluations. Although even after the entry into force of the draft Act, the implementation of sanctions in Estonia remains stratified between different institutions, the planned changes will help to clarify the legal space of Estonia, strengthen the competencies of the authorities and clarify the powers in the implementation and supervision of sanctions.

From the point of view of financial sanctions, the biggest change related to the draft Act is the expansion of the circle of persons with special obligations. In particular, this means an increase in the number of market participants who must have a risk mitigation and risk management system for sanctions. It is certainly worthwhile for all new persons with special obligations to take the new requirements seriously and invest in smart solutions. Especially since there seems to be a consensus that the use of financial sanctions to influence the conduct of third parties will continue to increase. It is also important to recall that the 12 sanction packages already adopted have directed the states and the obligated entities to be more proactive in their implementation, moving away from the more reactive and passive implementation of the past.

The cornerstone of an effective risk management system is an up-to-date risk assessment, the updating of which should be carried out by all persons with special obligations. Risk assessments should in particular consider new restrictions added in recent years, the updated FATF recommendations on the prevention of the financing of proliferation of weapons of mass destruction, and the risk environment that has changed beyond recognition. This is not an exhaustive list of factors to take into account when updating the risk assessment, but these keywords will certainly be relevant for the next two years.

Authorisations and supervisory observations

As of 31 December 2023 there were

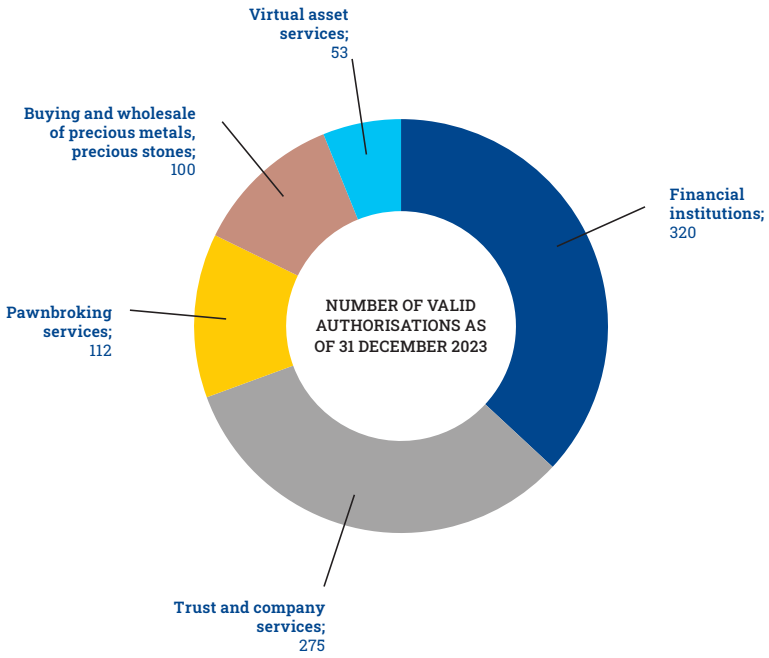
860

valid authorisations issued by the FIU

248

procedures for obtaining or amending an authorisation were completed

In 2023, the procedures for applications for amendments of authorisations arisen from amendments to the Money Laundering and Terrorist Financing Prevention Act were completed for the most part. In view of this, financial institutions and providers of company services emerged as the sectors with the largest number of authorisations.



Virtual asset service providers

As of 31 December 2023 **there were**

53
valid virtual asset service providers authorisations

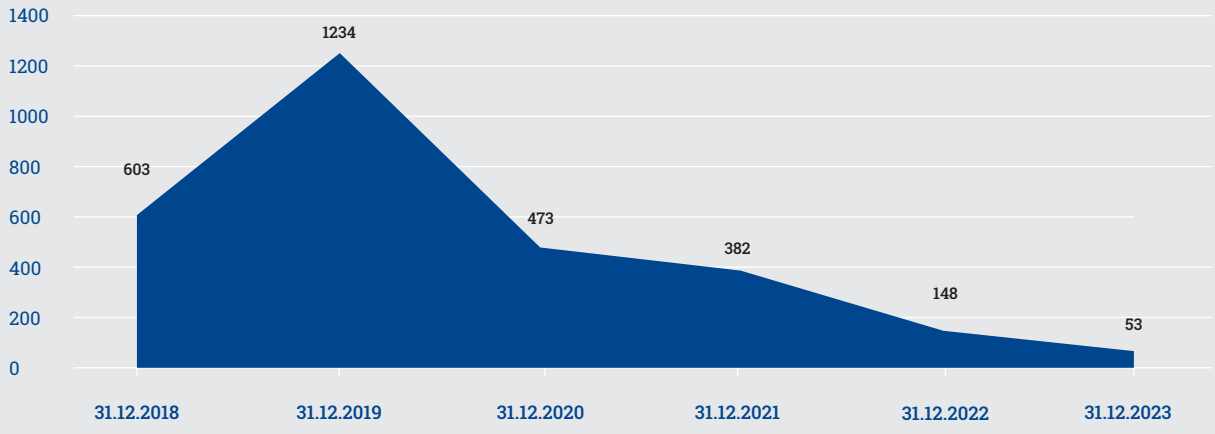
95
authorisations less compared to the beginning of the year

~500
authorisations less compared to the deadline of 15 June 2022 for compliance with the new requirements[8]

5
new authorisations were issued

162
applications for amending authorisations were processed

NUMBER OF COMPANIES AUTHORISED TO PROVIDE VIRTUAL ASSET SERVICES



For several years, the public has been able to see how the risks previously taken by Estonia accumulate and materialise in the sector of virtual asset service providers. Attention has also been paid to the steps that have been taken to tighten the requirements of service providers.

Having gone through this journey, the FIU has emerged as a competent spokesperson for the field, with many countries around the world inviting the FIU to provide advice or attend conferences. The FIU also provided its input into the International Monetary Fund's methodology for the risk assessment of virtual asset service providers.

[8] As of 10 March 2020, the FIU will issue a joint authorisation to provide virtual asset services instead of two separate authorisations (virtual currency wallet service and a service of exchanging virtual currency against a fiat currency). Thus, the number of companies offering virtual asset services and authorisations differs.

TIMELINE OF REORGANISATION OF THE VIRTUAL ASSET SERVICE PROVIDER SECTOR

JUUNI 2021

- **There were 641 valid authorisations** for virtual asset service providers. More than the EU total
- **Matis Mäeker** took over as the Head of the FIU established under the administration of the Ministry of Finance
- A repeat survey of virtual asset service providers and a risk assessment of company service providers were prepared **to clarify the national risk environment**
- 1/6 of the **foreign enquiries** were related to virtual asset service providers with Estonian authorisations; most of the information sent by the FIU was forwarded to competent authorities in other countries
- In the estimation of the FIU, the risk associated with virtual asset service providers required a rapid response, as the service providers have already been exploited and the risks **are gradually beginning to materialise.** The Head of the FIU noted that the choice is either a long-term market purge, where risks continue to materialise, or revocation of licences and their reprocessing and reissue
- For the first time the FIU **restricted crypto** assets at the request of another country
- The FIU warned of the materialising of financial risks, a year later, FTX, the world's largest crypto exchange, was declared bankrupt
- At the end of the year and at the beginning of the new year, the **United States**, in cooperation with the FIU, added two Estonian service providers who moved Russian criminal assets **to the sanctions list**

2022

- **382 authorisations** to provide virtual assets service; less than half comply with the reporting obligation
- Portals **warn against** Estonian service providers
- Russia's full-scale war in Ukraine brings with it **the risk of circumventing sanctions** using virtual currencies. The decline in serving Russian customers has lowered that risk. The FIU conducted 775 off-site inspections to assess the changed risks of service providers.
- The FIU prepared to grow its digital capacity to develop its strategic analysis function.
- On 15 March 2022, **the new requirements of the Money Laundering and Terrorist Financing Prevention Act** came into force. These were followed by **procedures conducted for applications** to amend authorisations and the assessment of documents submitted; additional **guidelines and training for service providers**
- 36 new **court cases** were initiated, half of which were related to authorisation procedures
- **10 supervisory procedures** were completed in which half of the inspected companies relinquished their own authorisation
- For the first time, the FIU set a **one-year restriction of disposal** on crypto assets.

2023

- 148 authorisations
- The state has been guided by the evaluation of MONEYVAL, the report of which focused, among other things, on the risks associated with virtual asset service providers.
- **A compliance notice** against 24 virtual asset service providers to align their own funds
- **167 recorded conversations** in the context of the authorisation process, which is twice as many as before
- Of the 85 new **court cases** against the FIU, a quarter are related to virtual asset service providers
- Of the 48 news stories that mentioned Estonia published in the FinTelegram portal within two years, 43 provided **negative information** about the virtual asset service providers authorised by Estonia
- At the end of December there were **53 valid authorisations for virtual asset service providers.** The procedure continues. There is still a step to take towards substantive on-site monitoring.

Of the nearly 100 authorisations for virtual asset service providers that expired in 2023, a third were declared invalid on the initiative of the FIU. In the remaining cases, the undertakings ceased their economic activity themselves, often only in the course of the authorisation amendment procedure, when they realised that they probably did not comply with the law.

CESSATION OF ECONOMIC ACTIVITY DURING THE AUTHORISATION AMENDMENT PROCEDURE

When changing the authorisation of the virtual currency service, it became clear that the Estonian members of the management board had left Estonia to live in a foreign country, and therefore they added an employee responsible for the company's IT field as a new member of the company's management board.

The FIU interviewed the new management board member who revealed that:

- the person took the new position for free
- no contract or benefits were offered when taking up the position of a management board member
- the current members of the management board were the new board member's friends and asked to take the position of the board member
- the management board member was interested in their previous IT work, but had no knowledge of company management or risks
- the new board member did not know the number of customers or the volume of transactions. When the FIU official showed the volume of transactions on paper, the board member could not count the number zeros, and only then started to comprehend the size of the transactions.

As a result of the interview, the FIU found that the change of the board member is fictitious, the new board member does not actually manage the company and the company's management board is not seated in Estonia.

The company relinquished its authorisation.

The main reasons for the revocation of the authorisation were:

The necessary documents to comply with the new requirements were not provided. In particular, business plans were deficient. The business plans of several companies overlapped, from financial forecasts to errors in logic and spelling, which pointed to fictitious documents.

The provision of the service was not commenced within six months of obtaining the authorisation. If an authorisation has been valid for several years, but a service is not provided, this may indicate that the company was created for sale. However, unknown future authorisation holders and their intentions are an increased risk.

The seat, place of activity and purpose of the management board of companies were not in Estonia. Although a member of the management board was appointed to Estonia, decisions of strategic importance were in fact taken by another member of the board living in a foreign country. Customer service, IT support, financial management and other personnel were located in foreign countries, and only a few employees in Estonia. The information shown on the websites also differed from the documents submitted to the FIU. For example, members of the Estonian management board were not included on the company's website, or the provision of the service was advertised to significantly wider jurisdictions than it was claimed to the FIU.

A virtual asset service provider with an Estonian authorisation at the end of 2023:

On average, the turnover per service provider was 404 million euros per year

5 employees on average

The main customers are from the United Kingdom, France, Curacao, the Marshall Islands and Estonia.

Of the 85 court cases that were initiated in 2023, nearly 20 involved virtual asset service providers. Some disputes also started with the company service providers and the application of non-compliance levies. Although in the light of the new requirements, a number of requests were not viable, many procedural actions were contested, up to the unlawfulness of the delay in the on-site inspection report. Although legal disputes are an integral part of the rule of law, a number of supervision subjects have a long way to go in understanding the role of a supervisory authority and the importance of high-quality dialogue to maintain long-term cooperation.

IMPECCABLE BUSINESS REPUTATION

A case of revocation of an authorisation in the absence of impeccable business reputation

Articles found in public sources refer to the illegal activities of an Estonian service provider in Russia.

According to a publicly available article, high-risk payment service providers gain access to the Western market through virtual asset service providers regulated in Estonia. The article mentions that the list of fraudulent companies operating with Estonian authorisations is long. The Estonian service provider in question allegedly enabled criminals (high-risk payment service providers) to operate in the financial market and to encourage cybercrime through virtual asset service providers.

Another article appears to refer to the involvement of the company in question with various scams.

The FIU determined that the company was related through a member of the management board to another company that had been under supervisory scrutiny of the FIU.

Public sources supported the information gathered in the proceedings.

The service provider's authorisation was revoked.

In the court case concerning the assessment of an impeccable business reputation, both the administrative court and the circuit court stressed the responsibility of the company to be convinced on their own of the impeccable business reputation of the member of the management board of the company. The applicant and holder of an authorisation must first of all ensure themselves that the members of their management bodies comply with the requirements of the law. How such compliance with requirements is arranged is at the discretion of the undertaking and its business risk.

The courts agreed with the FIU that the law does not provide for the possibility of testing through the FIU the suitability of different persons to start running a company engaged in the provision of virtual asset services. In this case, the appellant had the opportunity to submit a new and amended application for amendment of the authorisation after the FIU first established that the person designated by the appellant lacked an impeccable reputation. When the new application also did not meet the requirements of the law, it could be concluded that the appellant did not meet the circumstances of the object of inspection provided for by law. In such a situation where the appellant has already lost their credibility in the eyes of the FIU, it is no longer necessary to give them the opportunity to appoint another member of the management board and a liaison officer.

The Tallinn Circuit Court explained that the granting of an authorisation for virtual asset services requires that the credibility of the undertaking and its management board members is beyond doubt. Due to the hidden and complex nature of money laundering and terrorist financing, it is not sufficient to grant an authorisation to an undertaking whose credibility is uncertain but whose credibility can be assessed later in the course of supervision proceedings by the FIU. The credibility of an undertaking plays a very important role in ensuring that no terrorist financing or money laundering is carried out through the undertaking. The cited judgment of the administrative

and circuit court had not yet entered into force by the time the Yearbook was prepared.

The FIU will continue to pay close attention to companies understanding the real risk of their business activities and the implementation of corresponding measures in the supervision of market participants. The risk assessment is not only an important document when applying for an authorisation. If the turnover of a company's transactions, the number of customers or the volume of services provided increases or the geographical activity expands, then the company must also review its risk assessment and risk appetite accordingly. But even more importantly, the counter-measures of service providers, ie procedures as well as real human resources and technological solutions.

As a significant deficiency in the activities of virtual asset service providers, the Council of Europe's expert committee MONEYVAL pointed out, in line with the observations of the FIU, the inadequacy of the ability to establish the identity of the customer. Virtual asset service providers are a high-risk sector and a large proportion of their customers are non-residents, with higher risks of money laundering and terrorist financing. Knowing your real customers is one of the key factors in mitigating this risk. This is especially true at a time when deepfakes are on the rise.

By 1 January 2023, virtual asset service providers had to submit for the first time an audit firm's opinion regarding their own funds. Only 5%, ie eight, service providers with valid authorisations provided this opinion in due time. A compliance notice was issued to 90 service providers for the submission of an audit firm's opinion. As a result of the inspection, due to insufficient own funds, the FIU issued a compliance notice to 24 virtual asset service providers to align their own funds.

A COURT CASE THAT DRAWS ATTENTION TO APPLYING FOR AUTHORISATIONS AS A BUSINESS

On 28 June 2023, the Tallinn Circuit Court made a judgment in Administrative Case No 3-21-2139, which entered into force on 31 July 2023 and obliged the FIU to issue authorisations for virtual asset service providers retrospectively by default.

The FIU complied with the judgment by issuing eight authorisations by default.

By the end of 2023, the FIU revoked the authorisations once again, as the authorised companies did not bring their activities in line with the amendments to the Money Laundering and Terrorist Financing Prevention Act which had already entered into force on 15 March 2022.

CONTRIBUTION OF THE PRESS

In autumn, a series of articles was published in collaboration with the editorial boards of the investigative press of several countries that covered the virtual asset service providers operating in Estonia. The coverage revealed what fictitious facts have been submitted to the state to obtain or retain authorisations. Such articles are expected to call on the public to be vigilant about what information is worth checking from official public sources rather than blindly believing, and in whose hands to entrust your assets.

Such articles in Estonian and foreign media also show that the damage to the country's reputation is not going to end anytime soon. Foreign media portals continue to publish warnings about Estonian service providers for good reason.

EU Regulation 2023/1114 on markets in crypto-assets or MiCA

Whereas previously virtual asset service providers operated under the law of the respective Member State, the EU has now established uniform rules for market participants. This will allow the newly named crypto-asset service providers to offer their services under the same rules in all Member States.

As a result, it is no longer possible to submit an application with the FIU for an authorisation to provide a virtual currency service from 2025. Instead, it is necessary to submit an application with the Financial Supervision Authority for an authorisation to provide a crypto-asset service in accordance with the new requirements established in the Regulation.

Under the authorisation issued by the FIU, the virtual currency service can be provided until 1 January 2026.

Providers of company services

As of 31 December 2023, there were

275
valid authorisations for the provision of company services

39
authorisations less compared to the beginning of the year

5
new authorisations were issued

The FIU adheres to risk-based supervision, ie in particular, it looks at those sectors and market participants whose risks are highlighted by tactical and strategic analysis.

In 2022, providers of company services had a stronger showing in the risk analysis as a sector through which it is possible to conceal the beneficial owners of the business and members of the management body, and which is exploited in other countries to commit money laundering and related crimes.

In order to obtain additional information on risks and vulnerabilities and to plan supervised activities, the FIU sent out an off-site inspection questionnaire to 322 companies that had a valid authorisation to provide trust and company services.

The companies were asked for information on general data, internal control, internal audit, risk assessment, risk appetite, company customers, compliance with the reporting obligation and intermediaries used in business activities.

Although questionnaires are a world-renowned practice and a sign of good cooperation between the state and the private sector contributing data, in this case the response that followed involved both silence and disputes that reached the courts.

Out of 322 companies, 45 failed to comply with a repeated compliance notice to provide information and were fined a non-compliance levy for failing to provide data.

The FIU revoked the authorisations of 11 companies because they repeatedly failed to comply with compliance notices.

Nearly 30 service providers relinquished their authorisations because they realised they were not providing the service within the meaning of the Money Laundering and Terrorist Financing Prevention Act.

Eight service providers challenged the extent and reasonableness of the data they were asked to provide in court. In its judgment of 12 July 2023, the Tallinn Administrative Court found that the FIU has the right to request data and additional information from obliged entities in the course of exercising supervision to the extent determined by them. However, requesting information already available or available from public registers is not justified. As regards the lawfulness of the provision of information, the court pointed out that the need to collect and further process the data does not mean that there is no basis for requesting the information in this way. Under the Administrative Procedure Act, during proceedings in a matter, an administrative authority is required to establish the facts relevant to the matter and, if necessary, collect evidence on its own initiative for such purpose. In doing so, the administrative authority has the right to decide what data it considers relevant to the matter. This court judgment had not yet entered into force by the time the Yearbook was prepared, because the appellants lodged an appeal.

The results of the questionnaire showed that providers of trust and company services mainly provide address services and services related to the establishment of companies or transfer of shareholdings. Of the services that do not require an authorisation, most often services related to accounting are provided.

In 2022, of the 274 service providers the turnover related to company services amounted to 25 million euros, which represented on average just over 30% of their total turnover. For 49 service providers, company services accounted for the total turnover.

As of the end of 2022, nearly half of the service providers had no employees or had one employee. In contrast, companies' turnover per employee per year was significantly high, reaching more than 100,000 euros for eight companies. The small number of employees further increases the vulnerability of providers of company services, since in this case the resources would not be sufficient to implement due diligence measures.

MORE ATTENTION TO BENEFICIAL OWNERS

The supervision of providers of company services, similar to virtual asset service providers, has identified a lack of understanding of risk appetite and risk assessment. The vulnerability of this sector to money laundering, the financing of terrorism or weapons of mass destruction, as well as to circumvent financial sanctions, is heightened by the insufficient identification of the beneficial owners.

International standard-setter FATF estimates that providers of company services could be exploited by buying shelf companies from them to increase credibility and conceal the beneficial owners through a complex structure. This has also been identified by the FIU in previous supervision proceedings.

It often turned out that the service provider, when entering into a business relationship or making an occasional transaction, did not identify who the beneficial owner of the customer was. The FIU has identified situations in which the obliged entity was paid for the service by an intermediary and not by the customer. The service provider did not identify the relationship between the two companies, ie the customer and the intermediary, what was the purpose of such a transaction or who were the actual beneficiaries of the transaction. No due diligence measures were taken to identify the beneficial owners.

In connection with the Russian war in Ukraine, it is even more important to identify the beneficial owners, because attempts are also being made to hide persons or entities subject to restrictions behind complex ownership structures. Providers of company services may also be exploited without their own knowledge, but this can be prevented by high-level systems to mitigate the risks of money laundering and terrorist financing.

Financial institutions

As of 31 December 2023 there were

320
valid financial institution authorisations

30
authorisations more compared to the beginning of the year

11
new authorisations were issued

20
applications for obtaining authorisations and **20 applications for amendment of authorisations** were processed

Applications for obtaining or amending an authorisation often have an insufficient description of the service and a lack of knowledge of whether the authorisation of the FIU or the Financial Supervision Authority is required or the planned service does not require an authorisation at all.

A description often containing only a couple of words does not allow the processor to understand the content of the planned service and it remains unclear whether the applicant understands the conformity of their activities with measures to prevent money laundering and terrorist financing. The supervision revealed both those operating under a fake authorisation and those operating as small management companies which had received registration from the Financial Supervision Authority, but did not apply for the respective authorisation from the FIU. The discrepancies in the various registers will continue to be clarified in order to reflect the up-to-date picture of the Register of Economic Activities. Companies must also be careful to have a valid email address and contact person in the register in order to contact the company if necessary.

The FIU issues authorisations to operate as a financial institution for the following sub-categories:

- foreign exchange service providers (when providing a physical service)
- savings and loan associations
- lessors (for legal persons)
- lender (for legal persons)
- security and guarantee transaction service provider
- management company (which requires registration on the website of the Financial Supervision Authority)
- another financial institution within the meaning of the Credit Institutions Act

Other observations

SUITABILITY PROCEDURES

One of the tasks of the FIU is to assess the suitability of persons associated with authorised companies (management board, shareholders, beneficial owners, liaison officers) and the liaison officer of credit institutions and the person responsible for the international financial sanction for this position. A competent liaison officer ensures that systems for the prevention of money laundering and terrorist financing are in place and that more substantial and relevant reports are provided to the FIU. During the year, 61 reports regarding liaison officers were submitted.

Since 2023, the suitability procedure has become more thorough. Persons' previous work experience, education, training received, knowledge of their role, as well as the structure of the company where the person is employed are assessed. If necessary, the liaison officer candidate will be invited to the FIU for interviews, with the aim of ascertaining their knowledge, skills and suitability for this position.

As a positive trend and sign of good cooperation, the FIU is informed about the appointment of a liaison officer even if under the law the presence of a liaison officer is not mandatory.

SELECTION OF RECOMMENDATIONS FOR AUTHORISATION APPLICANTS AND OBLIGED ENTITIES

To prevent money laundering and terrorist financing, it is necessary to be aware of international requirements, guidelines, recommendations and typologies. There are requirements arising from national legislation to comply with, but it can only be effective in the fight against financial crime if this complex world is truly understood.

The FIU is open to dialogue with obliged entities, but this does not constitute legal advice. That is what impartial professionals, such as lawyers and attorneys-at-law, are there for.

Before applying for an authorisation, it is necessary to familiarise yourself with the national requirements as to whether and what type of authorisation the service requires, and to think carefully about your business plan and the content of the service. The applicant must clarify for themselves the main business concepts necessary for providing the service.

When applying for an authorisation, a precise and comprehensible description of the service must be provided, explaining, among other things, how and to which customers the service is provided. The company must carry out a legal analysis of what kind of authorisation is needed. Attach to the application a risk assessment and risk appetite prepared, relying on a specific company and the rules of procedure. This cannot be replaced by rather standard documentation often prepared and submitted by legal advisers.

Various providers of company services have brokered business authorisation applications for filing tax returns on behalf of customers, as is required by a foreign authority. In Estonia, this activity is not authorised.

Annual reports must be submitted in due time, since if delaying the submission of the report by more than six months, the company is considered to have ceased economic activity and this gives the FIU the right to revoke the authorisation.

PATH TO COOPERATION

MONEYAL's recommendation to raise market participants' understanding and awareness of the risks of countering money laundering and terrorist financing applies to all sectors, including non-financial institutions. In addition, the busy training activities that ended in 2023 were prompted by changes in law, Russia's ongoing military aggression in Ukraine and the consequent imposition of financial sanctions, as well as increased attention to the financing of terrorism.

In total, the FIU officials shared knowledge and experience with more than 5,000 participants from the private and public sectors, which is almost twice as many as before. Of the more than 30 information events in which the FIU participated, almost half of the organisers of the events were market participants, and the rest were either FIUs themselves or other state agencies.

Cooperation with umbrella organisations was also undertaken in the preparation of off-site inspection questionnaires for virtual asset service providers and gambling service providers. The questionnaires prepared in cooperation take into account the specificities of the sectors, the practical nuances, and are expected to be more understandable to the respondents along with their becoming known beforehand.

The questionnaire for virtual asset service providers was received in November 2023 by all companies that had an authorisation at that time. The deadline for responding was the end of February 2024. In April, however, in accordance with the new procedure, service providers will have to submit their first regular report on Eesti Pank's reporting portal. Continuous reporting also contributes to keeping the country's risk picture up to date.

Gambling service providers authorised by the Tax and Customs Board are also subject to supervision by the FIU within the meaning of the Money Laundering and Terrorist Financing Prevention Act. Both the use of cash and online gambling make the sector more vulnerable. To improve situational awareness, at the end of the year, all 31 companies holding an authorisation of a gambling service provider received a questionnaire for off-site inspection. The deadline for a response was February 2024.

About the Financial Intelligence Unit

With three years of operation as a separate government agency behind us, the FIU is changing gears.

Beside the challenges posed by the COVID pandemic and the Russian war of aggression, positions have been filled to a large extent, strategy has been updated, and internal process mappings and guidelines on work procedure have been prepared.

Strategic objectives of the FIU until 2026:

	Be the risk analysis centre and influencer of risk management in Estonia	**Implement more intelligent and digital solutions, and if needed, be an influencer of the public and private sector in the given field**	**Be the centre of competence for the prevention of money laundering and terrorism financing in Estonia**
FOR THIS THE FIU WILL:	Develop the capacity of strategic analysis and update the capacity of case analysis	Develop automated and contemporary risk analysis solutions	Guide the establishment of a system of money laundering and terrorism financing prevention in Estonia
	Initiate the relevant analysis and improve the existing ones	Cooperate with the public and private sectors, incl. universities and researchers	Continuously develop its own employees as well as train the public and private sectors
	Create efficiency indicators for constant evaluation of risk and control measures, and for the rapid mapping of changes		Be visible in Estonia as well as internationally and open to dialogue
	Apply itself and provide guidance for the execution of risk-based activities and applying measures in the state		Inform the public and private sectors about new trends and typologies as well as create relevant manuals

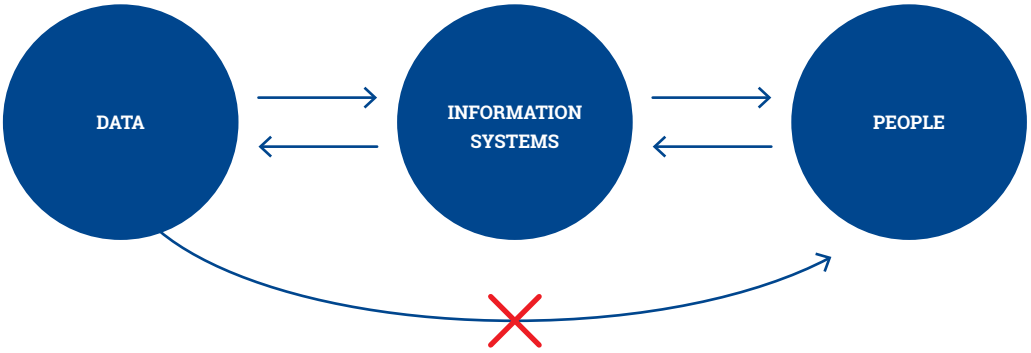
The increase in staff was essential to fulfil the tasks assigned to the FIU under several laws and official agreements. All in all, it has become a comparatively young and purposeful team. An organisation that has grown in size also needs quality management. Thus, managers at all levels of the FIU underwent a development programme consisting of five modules. In addition, officials participated in training courses and collaborative projects offering a wide range of professional skills and knowledge, many of which were aimed at developing data analysis capabilities – from peer-to-peer exchange of knowledge to international forms of cooperation.

THE IMPORTANCE OF MACHINE PROCESSING OF DATA

One of the strategic objectives of the FIU is the development of digital capabilities. This is closely linked to the goal of being a smart risk-seer. The International Monetary Fund's (IMF's) analysis of the prevention of money laundering in the Nordic and Baltic countries also suggested investing in high-tech data analytics.

To the FIU, automation, integration and reliable data will be the information technology keywords for the next two years.

The integral components of information technology are data, information systems and people. It is important to contribute to the development of all three values, because all three are constantly changing over time and interdependent.



Increasingly large amounts of data and technological advances characterise both law-abiding and criminal forces alike. The only way to be successful in this struggle is to significantly increase the share of machine-reliance in data processing.

Data is the FIU's cornerstone, the quality and reliability of which we increase through the creation of a data exchange portal. This creates an effective communication channel between the institution and the private sector for the exchange of information and the prevention of money laundering and terrorist financing. The project will also develop a new reporting system in cooperation with the private sector, taking into account best international practices and the long-term experience of the FIU. The application of AI in risk assessment, prioritisation and decision-making needs to be continued. In doing so, it is important to integrate systems to ensure secure and efficient data exchange both within the institution and with partners.

The development work of the strategic analysis function has reached the stage that it is gradually becoming more visible both inside and outside the FIU, allowing for significantly more efficient use of data. It brings a larger number of users closer to data, creates more value from mass data, and enhances the ability to find hidden messages in the data. In practice, this means flexible management reports for managers at every level of the FIU, faster pre-analysed information and a more detailed risk picture for the analyst – both on a specific case and across different areas as a whole.

Just like the prevention of money laundering, the leap in the development of the strategic analysis function requires good cooperation from above and between authorities. In return, all parties benefit from an informed and up-to-date risk picture.

STRIVING TO BE A STEP AHEAD

From the steps taken in the daily work of the officials, the values of the organisation also took shape. **The FIU and its officials are:**

Trustworthy

We fight financial crime together with our partners from both the private and public sectors, and this entire network is based on honesty and trust. The information provided to us is protected and we use it to keep guard over the integrity of financial transactions. We are visible and with our competence we show the direction in the prevention of money laundering and terrorist financing in Estonia. In our working family, we trust each other.

Decisive

We are bold in our actions and are not afraid to make difficult decisions. We act purposefully and efficiently and we dare to be innovative, think outside the box and dream big while doing our job. We are guided by laws, our mission and our sense of justice. Every member of our working family prevents financial crime – their actions are decisive and have an impact.

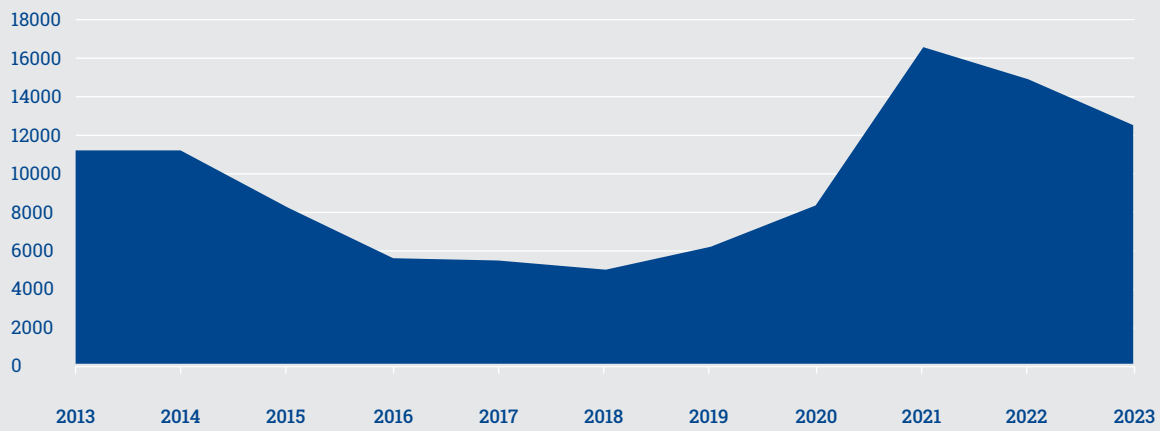
Intelligent

In the fight against financial crime, we often face professionals, so we need to be smarter ourselves and use the best practices and technology. We are developing ourselves, our field of work and the entire system of money laundering and terrorist financing prevention in Estonia, we are an example and a guide for others. Our working family values continuous development. It includes the best in Estonia and the world with experience, as well as young people who are just starting out – we all learn from each other.

The vision of the FIU is to be a step ahead in guarding the honesty of financial transactions. Of whom or what – that's what the 2023 Yearbook was talking about.

2023 in numbers

Number of reports



Reports by type and sector

Sector	Suspicious transaction report (STR)	Unusual transaction report (UTR)	Unusual activity report (UAR)	International sanctions report (ISR)	Terrorist financing risk (TFR-1) and suspicion (TFR-2) report	Inquiry	Cash transaction report (CTR)	Total
Credit institution	4392	289	658	430	82		3	**5854**
Virtual asset service provider	2597	156	504	52	121			**3430**
Financial institution	191	66	146	31	56		686	**1176**
State agencies	49	10	10	55	4	61	66	**255**
Foreign entities and persons	11		1	6	1	552		**571**
Gambling operators	140	21	5				338	**504**
Professionals (legal services, audit, etc)	53	69	35	16	8		177	**358**
Other private operators	16	76	12	5	1		97	**207**
Not an obliged entity	113	4	11	11			6	**145**
Total	**7562**	**691**	**1382**	**606**	**273**	**613**	**1373**	**12500**

DISCLOSURES AND DISPOSAL RESTRICTIONS

12 500

reports

150

disclosures to investigative authorities, plus 610 factual data transmissions to the police information system

113

disposal restrictions

30-day restrictions
in 28 cases

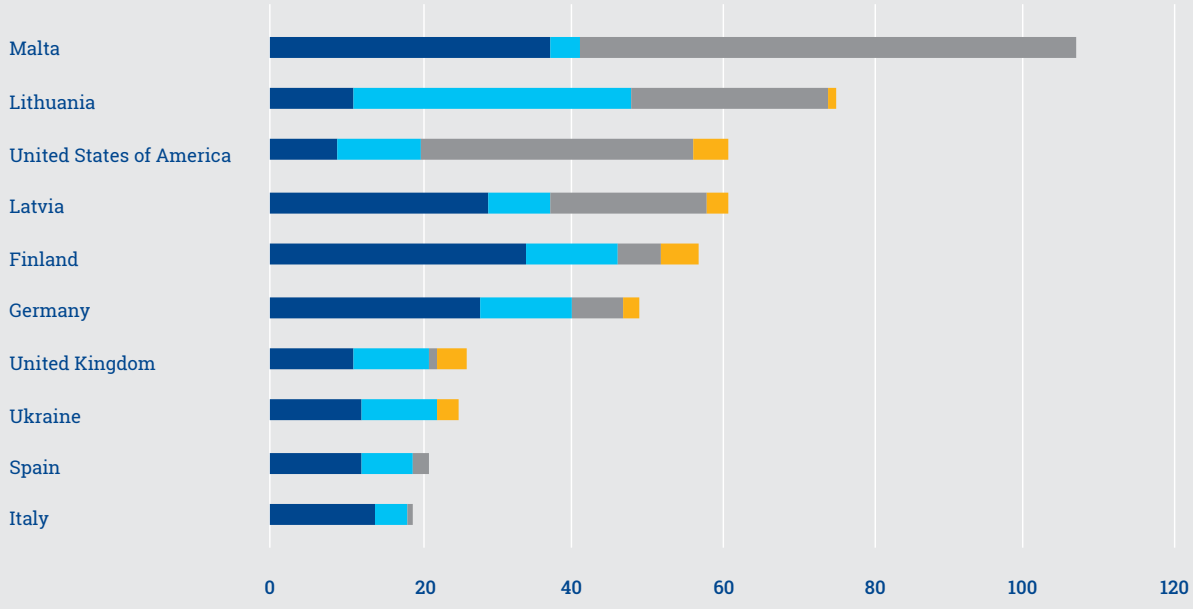
totalling €4.37 million
60-day restrictions
in 50 cases

totalling €9.45 million
1-year restrictions in 35 cases
totalling €3.85 million

20

compliance notices for transfer to state ownership totalling nearly €1.36 million

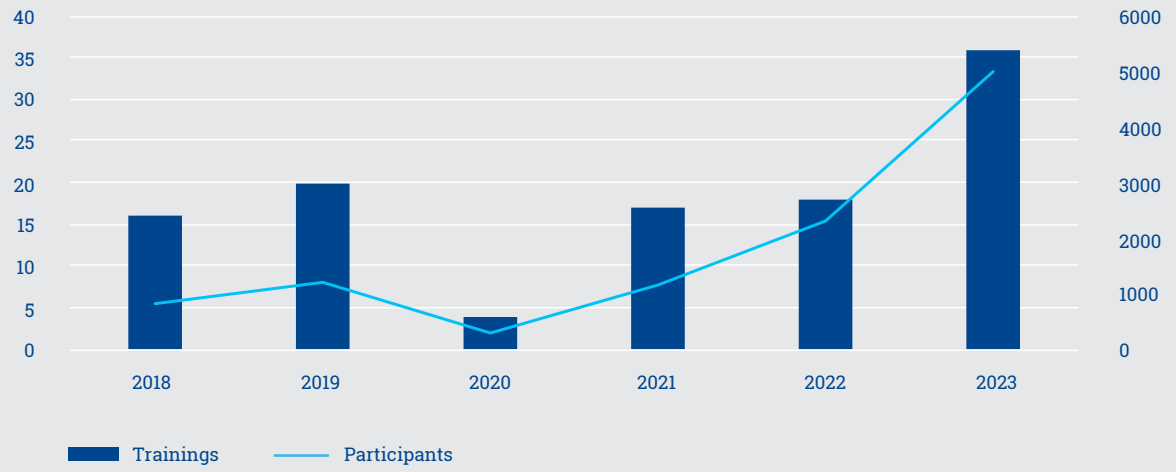
THE MOST COOPERATIVE FOREIGN FIUS



APPLICATION OF FINANCIAL SANCTIONS

		Measure applied as of 31 December 2023	
Regime	**Subject of sanction, related person**	**Frozen**	**Not made available and deposit limit**
EL nr 2016/44 Libya	Aleksandr Sergeevich Kuznetsiv	249	-
EL nr 2018/1542 Use of chemical weapons	Vladimir Alexandrovich Panyaev	10	-
EL nr 2580/2001 Combating terrorism	Palestiina Islami Džihaad	8 205	-
EU No 269/2014 Russia	Andrey Igorevich Melnichenko / Aleksandra Melnichenko	28 146 798	30 398
EU No 269/2014 Russia	Alexey Alexandrovits Mordashov	1 064	-
EU No 269/2014 Russia	Alexey Gennadyevich Nechayev	52 123	12
EU No 269/2014 Russia	Viatcheslav Moshe Kantor	4 981 406	3 042
EU No 269/2014 Russia	VTB Bank	2 925	800
EU No 269/2014 Russia	Public joint-stock company Rosbank	15 050	-
EU No 269/2014 Russia	Petr Olegovich Aven; Mikhail Maratovich Fridman; German Borisovich Khan; Alexey Viktorovich	3 501	-
EU No 269/2014 Russia	Elena Petrovna Timchenko	-	5 840
EU No 269/2014 Russia	Igor Aleksandrovich Ananskikh	6 035	-
EU No 269/2014 Russia	Igor Albertovich Kesaev	-	12 325
EU No 269/2014 Russia	Victor Vladimirovich Soyko	-	1 700
EU No 269/2014 Russia	Federal State Unitary Enterprise Rossiya Segodnya International Information Agency	4 379	-
EU No 269/2014 Russia	Sergei Borisovich Ivanov	-	1 500
EU No 269/2014 Russia	Aleksandr Yurievich Timofeev	-	1 000
EU No 269/2014 Russia	Ruslan Gadzhievich Gadzhiyev	-	1 000
EU No 269/2014 Russia	Bank Rossiya	302	-
EU No 269/2014 Russia	ANO TV-Novosti	-	790
EU No 269/2014 Russia	Alexander Petrovich Petrov	-	290
EU No 269/2014 Russia	Marina Magomednebiyevna Akhmedova	-	150
EU No 269/2014 Russia	Yelena Alekseyevna Perminova	40	-
EU No 269/2014 Russia	Yury Petrovich Sinekshchikov	25	-
EU No 269/2014 Russia	Sergey Anatolevich Gavrilov	-	60
EU No 269/2014 Russia	Andrey Zhuk	-	151
EU No 269/2014 Russia	Gleb Leonidovich Mikhailov	-	86
EU No 269/2014 Russia	Dmitriy Vladimirovich Shmelev	-	54
EU No 269/2014 Russia	Maksim Evgenyevich Ivanov	-	32
EU No 269/2014 Russia	Natalya Anatolyevna Pshenichnaya	-	23
EU No 269/2014 Russia	Alexey Nikolaevich Mikhaylov	-	47
EU No 269/2014 Russia	Aleksey Aleksandrovich Petrov	-	15
EU No 269/2014 Russia	Alexander Vladimirovich Novikov	-	15
EU No 269/2014 Russia	Vladimir Sergeevich Petrov	-	6
EU No 269/2014 Russia	Maksim Evgenyevich Ivanov	-	2
EU No 269/2014 Russia	Vladimir Petrovich Kononov	100	-
EU No 833/2014 Russia	Russian citizens (subject to 100,000 deposit limit)	-	197 530
	KOKKU	**33 222 212 €**	**256 868 €**

TRAININGS, INFORMATION EVENTS



REFERENCES AND FURTHER READING

Anti-money laundering and counter-terrorist financing measures. Estonia. Fifth Round Mutual Evaluation Report. Committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL), 2022.
https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd96

Nordic-Baltic Regional Report: Technical Assistance Report-Nordic-Baltic Technical Assistance Project Financial Flows Analysis, AML/CFT Supervision, and Financial Stability. International Monetary Fund, 2023.
https://www.imf.org/en/Publications/CR/Issues/2023/09/01/Nordic-Baltic-Regional-Report-Technical-Assistance-Report-Nordic-Baltic-Technical-538762

The Other Side of the Coin. European Union Financial and Economic Crime Threat Assessment (EFECTA). Europol, 2023.
https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf

Prosecutor's Office Yearbook 2023.
https://aastaraamat.prokuratuur.ee

Report on Abuse of Virtual Assets for Terrorist Financing Purposes.
Information Exchange Working Group (IEWG). Egmont Group, June 2023.

UN. Panel of Experts Established pursuant to Security Council Resolution 1973 (2011).
Letter dated 5 September 2018 from the Panel of Experts on Libya Established pursuant to Resolution 1973 (2011) addressed to the President of the Security Council. [New York] : UN, 5 Sept. 2018.
https://digitallibrary.un.org/record/1640692?v=pdf

SURVEYS AND TYPOLOGY NOTICES OF THE FINANCIAL INTELLIGENCE UNIT

Survey 'Financing models of the terrorist organisation Hamas', 2024. Summary in English.
https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#financing-models-of-

Survey 'Cash-related risks of money laundering and terrorist financing in Estonia', 2023. Summary in English.
https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#cash-related-risks-o

Survey 'Licit and illicit cash flows in the Baltic States'. Estonian, Latvian and Lithuanian financial intelligence units, 2023.
https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#licit-and-illicit-ca

Short study 'Sanctions evasion through the use of virtual currencies', 2023.
https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#sanctions-evasion-th

Overview of the foreign inquiries sent to the Estonian FIU in 2022.
https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#foreign-inquiries-se

Typology notice 7TT202401. The use of Estonian legal persons linked to Russian and Belarusian persons to evade sanctions. In Estonian. https://fiu.ee/aastaraamatud-ja-uuringud/tupoloogiateated#tupoloogiateade-7tt2

Typology notice 7TT202309. The use of payment cards to evade sanctions. In Estonian.
https://fiu.ee/aastaraamatud-ja-uuringud/tupoloogiateated#tupoloogiateade-7tt2--2

Typology notice 4TT202305. Trade-based money laundering. In Estonian.
https://fiu.ee/aastaraamatud-ja-uuringud/tupoloogiateated#tupoloogiateade-4tt2

GUIDELINES PUBLISHED BY THE FIU IN 2023

Recommendations for virtual asset service providers. In Estonian.
https://fiu.ee/uudised/rahapesu-andmeburoo-soovitused-virtuaalvaaringu-teenuse-pakkujatele

Recommendations for trust and company service providers. In Estonian.
https://fiu.ee/tegevusluba-ja-jarelevalve/usaldushaldus-ja-ariuhinguteenus#soovitused-turuosali

Detecting and Preventing Sanctions Evasion and Circumvention in Trade.
Practical Guidance for Economic Operators by the competent authorities of Estonia, Latvia, Lithuania and Poland.
https://fiu.ee/en/guidelines-fiu/guidelines#recommended-guidelin

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