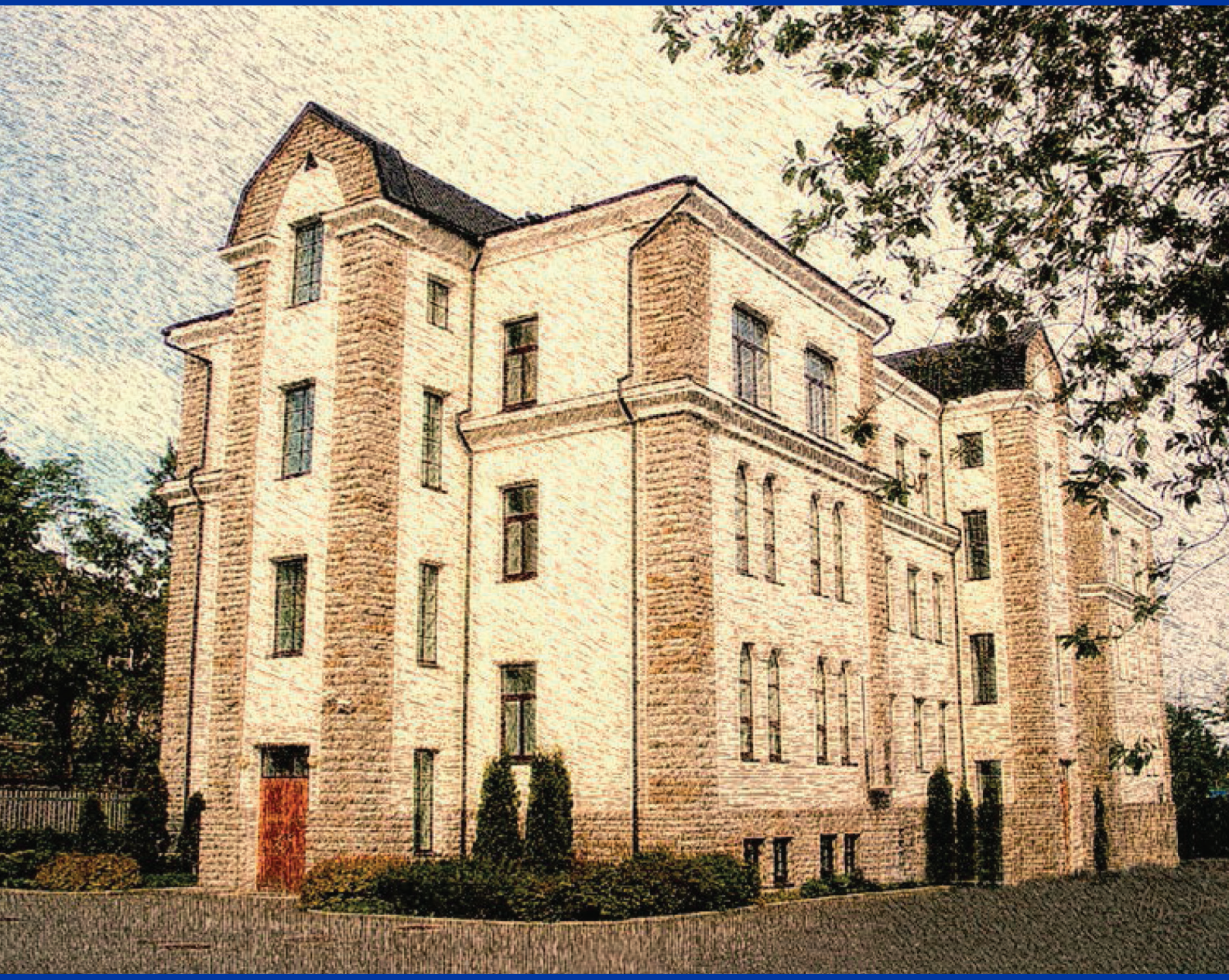
ESTONIAN FIU



YEARBOOK 2019

OVERVIEW OF THE ACTIVITIES OF THE ESTONIAN FINANCIAL INTELLIGENCE UNIT IN 2019

TALLINN 2020

CONTENTS

FOREWORD 4

1. THE YEAR 2019 IN THE ESTONIAN ANTI-MONEY LAUNDERING SYSTEM 5

1.1. Legislative changes 5

1.2. New information system of the Financial Intelligence 6

2. OVERVIEW OF THE PERFORMANCE OF THE FINANCIAL INTELLIGENCE UNIT IN 2019 7

2.1. Overview of the reports received by the FIU and their analysis 7

2.2. National and international cooperation 12

2.3. Supervision 16

2.4. Granting of authorisations 17

3. COURT DECISIONS ON MONEY LAUNDERING CASES IN 2019 19

3.1. Criminal proceedings 19

3.2. Administrative court proceedings 21

4. MONEY LAUNDERING SCHEMES 22

5. INTERNATIONAL FINANCIAL SANCTIONS 27

6. LOOKING AHEAD TO 2020
29

FOREWORD

In 2019, there were a number of important developments in the prevention of money laundering and terrorist financing, which we will discuss in this yearbook.

The number of virtual currency service providers continued to grow very rapidly and the risks associated with it increased in 2019. Last December, the Estonian Parliament adopted a first set of amendments to address major shortcomings in the regulation of virtual currency service providers. This is a first step in the right direction and we expect policy-makers and legislators to continue their efforts in this area.

In 2019, we replaced our information system and moved it to a new platform that enables new modern functionalities. We significantly updated the environment for sending reports intended for obliged entities and revised the classification and indicators of reports.

At the end of 2019, the implementation of EU financial sanctions in the case of Rossiya Segodnya became public and received great attention in Estonia. So far, the case has been challenged before the court and we are awaiting the court's assessment.

International information exchange continued to grow in 2019. We were able to help our external partners with the information required in several noteworthy cases. Thanks to the information from our foreign partners, we were able to provide many Estonian criminal proceedings with important information on financial transactions and predicate offences committed abroad.

The number of terrorist attacks in European countries has fallen significantly over the past two years. However, this does not mean a reduction in the challenges of identifying payments related to terrorist financing.

In 2019, many cases related to cyber fraud attracted the attention of the Financial Intelligence Unit. The FIU also analysed a number of cases involving Estonian service providers and the domestic laundering of assets obtained from crimes committed abroad.

The following chapters of this yearbook provide a closer look at these and other topics.

Madis Reimand
Head of the Financial Intelligence Unit

1. THE YEAR 2019 IN THE ESTONIAN ANTI-MONEY LAUNDERING SYSTEM

1.1. LEGISLATIVE CHANGES

Just before the end of 2019, the Act on Amendments to the Money Laundering and Terrorist Financing Prevention Act and the State Fees Act (8 SE) was promulgated. The amendments entered into force on 10 March 2020. Persons that already hold an authorisation must comply with the new requirements by 1 July 2020 at the latest.

Legislative changes are essential for the AML/CFT system as they tighten the requirements for authorisation and provision of virtual currency services. The Financial Intelligence Unit indicated the need to make such changes already in 2018. The changes will contribute to the quality of service provision and mitigate the risk of individuals falling victim to fraud in this sector. In addition, the potential damage to the reputation of the Estonian State will decrease. The most important amendments are the following:

1. the concept of a virtual currency service was harmonised;
2. the provision of a service for exchanging a virtual currency against another virtual currency was also included among the services subject to authorisation;
3. mandatory AML/CFT requirements and due diligence applicable to the provision of virtual currency services were equated with financial institutions.

In 2019, the Financial Intelligence Unit identified a scheme in which money was laundered by taking advantage of bankruptcy proceedings. Pursuant to section 45 of the Bankruptcy Act, all seizures of assets are terminated upon the declaration of bankruptcy. This also includes seizures in criminal proceedings which jeopardises the preservation of property during criminal proceedings. The FIU also informed the Ministry of Justice about the loophole in the law, and the scheme is described in further detail in section 2.1 of the yearbook.

1.2. NEW INFORMATION SYSTEM OF THE FINANCIAL INTELLIGENCE

The Financial Intelligence Unit introduced a new information system in 2019. The previous information system was outdated in terms of both the platform and its functionalities. The new information system addressed some important functional needs and, above all, the transition to the new platform provided a basis for the development of further modern functionalities. It is now significantly easier for obliged entities to send reports via an online form, where they can use templates for the most common types of reports, save and later continue pending reports, determine report types and suspicion indicators through a new system of indicators. Since the end of the year, it is also possible to report online in English.

As a result of the good cooperation between the FIU and the development team of the IT and Development Centre at the Ministry of the Interior (SMIT), a number of important developments were carried out by the end of the year. Obliged entities can now send reports directly from the system to the system (from computer to computer) in xml format by developing IT solutions for their information system. At the end of 2019, two market participants had such developments in place. Several developments were aimed at making the information system more usable as a tool for the FIU officials.

2. OVERVIEW OF THE PERFORMANCE OF THE FINANCIAL INTELLIGENCE UNIT IN 2019

2.1. OVERVIEW OF THE REPORTS RECEIVED BY THE FIU AND THEIR ANALYSIS

Since the beginning of 2020, the Financial Intelligence Unit (FIU) has been using a new methodology for the statistics on reports, and thus the figures will differ slightly from those published in previous yearbooks. There were a number of changes to the methodology. Firstly, reports received through cross-border dissemination (XBD) are no longer included in the list of reports. Secondly, while the number of reports in previous yearbooks was calculated on the basis of the date of registration of the report in the FIU, from 2020 onwards the date on which the report was sent to the FIU will be used as the basis. In addition, the system of types and indicators of suspicion was fundamentally changed. With the transition to the new system, the information on the indicators is not fully comparable to previous years.

As in the past, reports are subdivided by sum and suspicion, with the latter containing not only suspected money laundering, suspected terrorist financing and suspected international sanctions, but also inquiries. Since mid-2019, in the case of reports that concern money laundering, a distinction has been made between suspicious transaction reports (STRs), unusual transaction reports (UTRs) and unusual activity reports (UARs). For reports related to terrorist financing, a distinction is made between reports related to unusual transactions (TF_UAR) and reports related to suspected terrorist financing (TFR). In May 2019, the FIU published an updated guideline on the characteristics of suspicious transactions, which can be found in the guidelines section on the FIU's website: https://www.politsei.ee/en/guidelines.

In 2019, the FIU received 6164 reports (Figure 1), which exceeds the number of reports in 2018 by over a thousand.

In addition, the number of reports sent through cross-border dissemination, or XBDs, increased exponentially: while there were 20 such reports in 2017 and about 1700 in 2018, there were more than 4000 in 2019 (Figure 2).

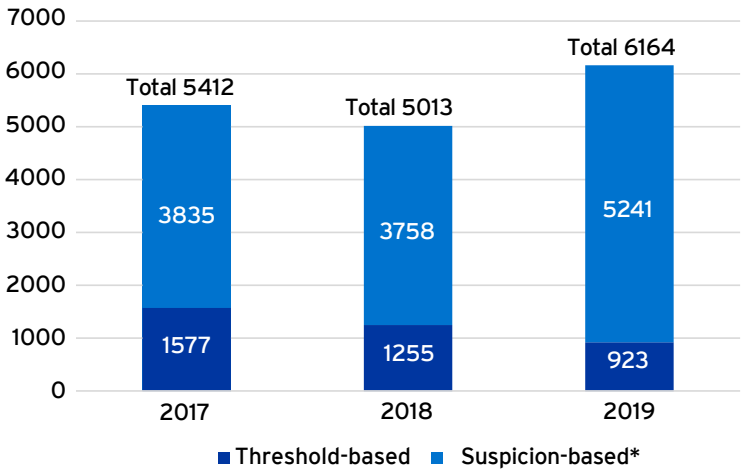


Figure 1. The number of reports received by the FIU between 2017–2019

Note: threshold-based reports also include those where the reason for sending the report is not stated. Suspicion-based reports also include inquiries.

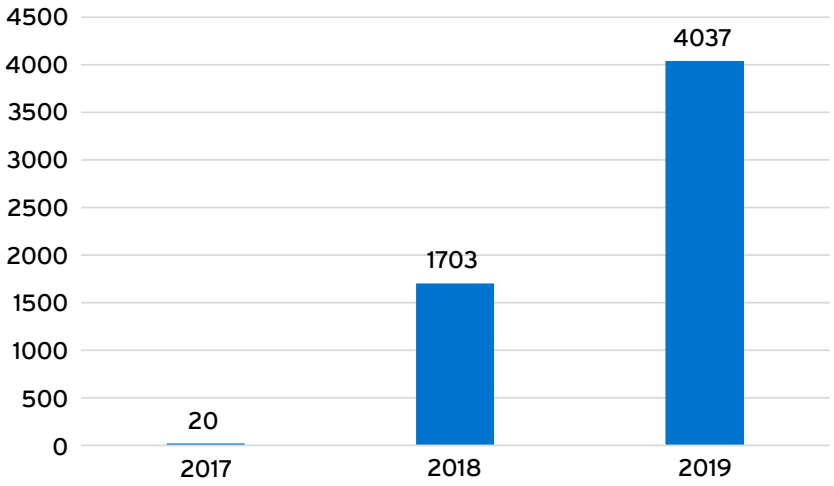


Figure 2. The number of XBDs received by the FIU between 2017–2019

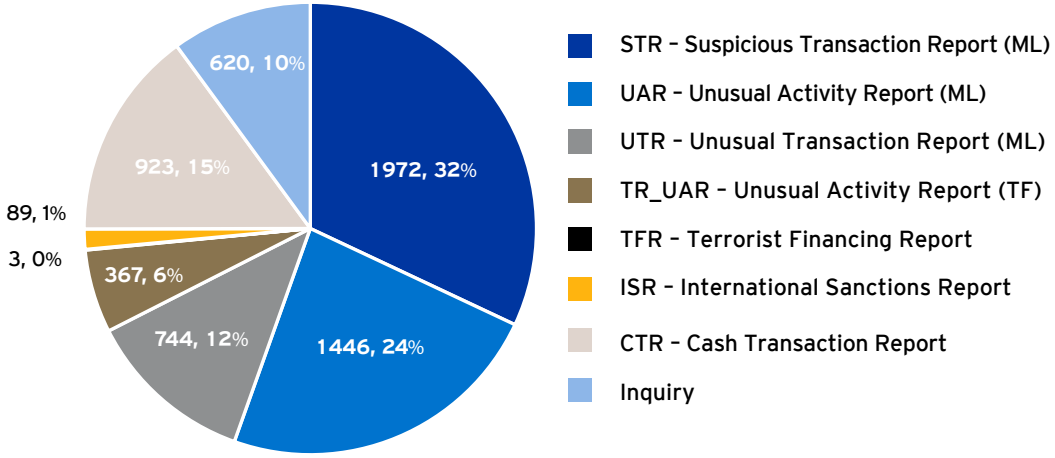


Figure 3. Distribution of reports based on suspicion and sum in 2019

75% of the reports received in 2019 were suspicion-based, 15% were cash transaction reports and one tenth were inquiries (Figure 3). Suspicion-based reports were dominated by reports of suspected money laundering — suspicious transaction reports, unusual transaction reports and unusual activity reports (STR, UTR and UAR). There were 370 terrorist financing reports and 88 reports on suspicion of being subject to the International Sanctions Act.

As in previous years, the majority of the reports sent to the FIU in 2019 came from credit and financial institutions (Table 1). Over the past three years, the number and share of the reports sent by credit institutions, gambling operators and foreign authorities have increased, while the share of reports sent by financial institutions has decreased. The reporting activity of credit institutions, gambling operators and notaries increased significantly in 2019 compared to the previous year (the FIU received 168 reports from notaries in 2018 and 394 reports in 2019).

Table 1. Distribution of reports received by the FIU based on senders between 2017–2019

	2017		2018		2019	
	No. of reports	% of senders	No. of reports	% of senders	No. of reports	% of senders
Credit institutions	2317	42,8	2208	44,1	2905	47,1
Financial institutions	1865	34,5	1360	27,1	1188	19,3
Providers of virtual currency services	3	0,1	7	0,1	400	6,5
Gambling operators	321	5,9	279	5,6	250	4,1
Other obliged entities	47	0,9	85	1,7	75	1,2
Foreign authorities and persons	357	6,6	541	10,8	519	8,4
State authorities	274	5,1	266	5,3	231	3,7
Professionals	207	3,8	223	4,4	506	8,2
Non-obliged entities	21	0,4	43	0,9	90	1,5
TOTAL	**5412**	**100**	**5012**	**100**	**6164**	**100**

Table 2. Distribution of reports sent to the FIU in 2019 based on the reason for sending and the sender

Sender	STR	UAR	UTR	TF_UTR	TFR	ISR	CTR	Inquiry	Total
Credit institutions	1250	1082	488	3	2	77	3		2905
Financial institutions	143	237	108	201		2	497		1188
Providers of virtual currency services	324	55	19	1			1		400
Gambling operators	5	4	6	75		1	159		250
Other obliged entities	10	3		5		1	56		75
Professionals	97	21	119	81	1	3	184		506
... Attorneys	8								8
... Auditors	2	3	7	1			49		62
... Financial advisors and tax advisors	1	4	1						6
... Bailiffs	1		1				1		3
... Other legal advisors	2	4	3		1				10
... Notaries	77	7	104	80		3	123		394
... Bankruptcy trustees	1						1		2
... Providers of accounting services	4	3	3				10		20
... Trust and company service providers	1								
State authorities	51	13	4	1		3	24	135	231
Foreign authorities and persons	21	12				1		485	519
Non-obliged entities	70	19				1			90
TOTAL	**1971**	**1446**	**744**	**367**	**3**	**89**	**924**	**620**	**6164**

Note: STR – suspicious transaction report; UAR – unusual activity report; UTR – unusual transaction report; UTR TF – unusual transaction report with reference to the suspicion of terrorist financing; TFR – terrorist financing report; ISR – international sanctions report; CTR – cash transaction report.

In 2019, credit institutions clearly dominated as senders of reports related to money laundering. Most of the reports on terrorist financing were sent by financial institutions in relation to transactions made with countries with high risk of terrorist financing or persons originating from such countries (unusual transaction reports or UTRs). The majority of threshold-based reports were also sent by financial institutions. There have been no significant changes in these trends in recent years.

In 2019, the most common reason for sending a money laundering suspicion report was an unusual transaction in an account (Figure 4), followed by the fact that a person was suspected of money laundering or did not provide sufficient explanations to comply with due diligence measures.

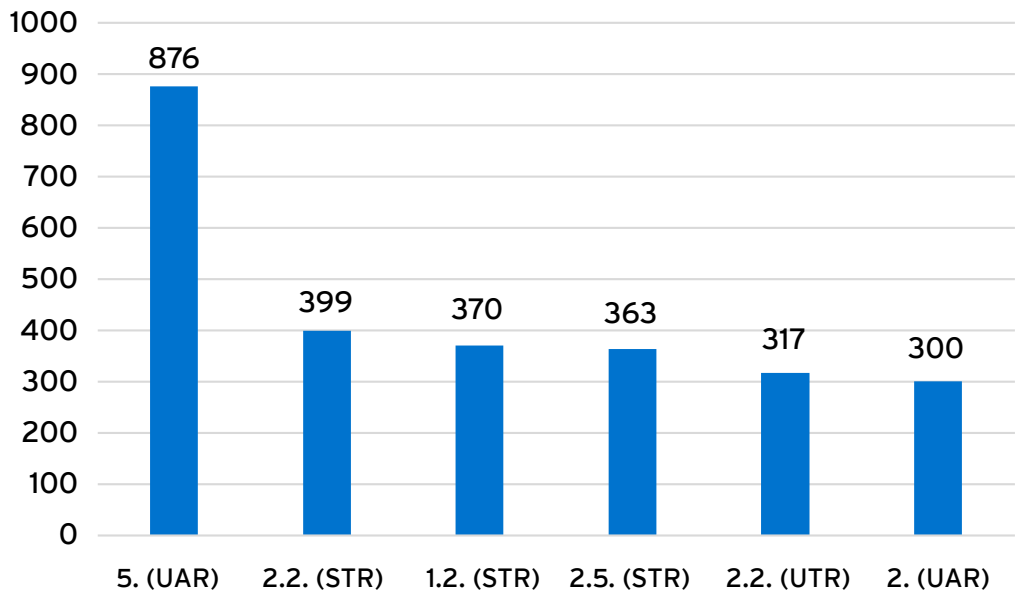


Figure 4. The main reasons for reporting suspected money laundering in 2019

Note:
5. (UAR) Unusual transactions in an account
2.2. (STR) There is a previously existing suspicion, or the application of due diligence measures has led to a suspicion of the person being involved in money laundering
1.2. (STR) There are grounds to believe that the person has provided falsified information
2.5. (STR) The person does not submit explanations or documents regarding the transaction to the extent necessary to perform due diligence measures or the information provided is not plausible (subsection 42 (1) occasional transaction and subsection 43 (1) transaction of a person in a customer relationship of the Money Laundering and Terrorist Financing Prevention Act)
2.2. (UTR) An unusual transaction in an account
2. (UAR) Unusual cash transactions not related to the usual economic activity of the person

Restrictions on the disposal of property

The FIU has the right to suspend or restrict the disposal of assets in case of suspicion of money laundering or terrorist financing. In 2019, the FIU restricted the use of a person's account for 30 days on 37 occasions and for 60 days on 31 occasions (Figure 5). The total volume of assets subject to the restrictions imposed by the FIU was more than 30 million euros. On 11 occasions, property with a total worth of more than 1.9 million euros was retained by a court order in criminal proceedings.

In addition to the restrictions of bank accounts, the FIU imposed two restrictions on the disposal of cash totalling 93,000 euros, on the disposal of more than 1,500 prepaid cards, on the disposal of several immovable properties and on transactions related to shares and the transfer of immovable property between companies.

In 2019, the FIU twice imposed restrictions on the disposal of assets for a period of up to one year.

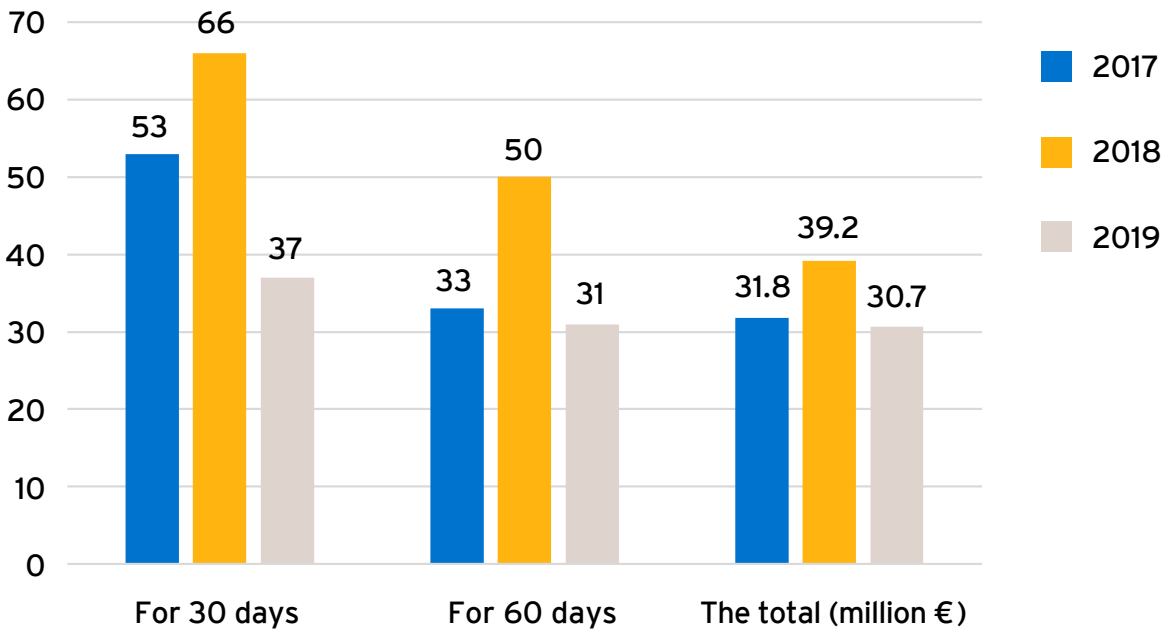


Figure 5. Restrictions on the disposal of bank accounts imposed by the FIU between 2017–2019

Case 1

The restriction was imposed due to the intention to use the provisions of the Bankruptcy Act for money laundering. A company initiated bankruptcy proceedings against another company, both with the same owner. The purpose of the bankruptcy proceedings was to take advantage of section 45 of the Bankruptcy Act, since the seizure previously imposed in criminal proceedings must be terminated after the declaration of bankruptcy on the basis of the said provision. As a result, the seizure of property in criminal proceedings was terminated and there was a risk that the persons suspected of having committed a criminal offence would take possession of the property, which was a subject of suspicion of a criminal offence, making it possible to complete the money laundering process, irrespective of the criminal proceedings being conducted.

Time-limits: With the permission of the court, the FIU set it in June 2019. The restriction applies until the legal ownership of the assets has been established, but for no longer than 1 year.

The restricted amount was 150,000 euros.

Case 2

The criminal proceedings were terminated because the perpetrators of a business e-mail compromise (BEC) scheme could not be identified. There was a risk that if the FIU did not impose a restriction, the assets would fall into the hands of persons whose ownership rights were under suspicion by the FIU under the Money Laundering and Terrorist Financing Prevention Act.

Time-limits: The FIU set a restriction in October 2019. The restriction applies until the legal ownership of the asset has been established, but for no longer than six months.

The restricted amount was around 40,000 euros.

2.2. NATIONAL AND INTERNATIONAL COOPERATION

One of the tasks of the Financial Intelligence Unit (FIU) is to cooperate with obliged entities as providers of information, as well as with competent supervisory and investigative bodies as consumers of information. Its purpose is to prevent money laundering and terrorist financing. The role of the FIU is to act as a filter between the private sector and law enforcement authorities. When the FIU receives information about suspicious or unusual transactions and activities carried out using obliged entities, the FIU analyses the information received in order to identify possible signs of criminal activity. In general, the principle of cooperation of the FIU is to identify and communicate the information necessary for pre-trial investigations in cases of money laundering or terrorist financing and related criminal offences.

As in previous years, officials of the FIU provided methodological support and organised various training activities for obliged entities and market participants in 2019. Overall, in 2019 officials of the FIU organised 20 anti-money laundering training activities with more than 1200 participants (Table 3). In addition to the staff of the obliged entities, the cadets of the Estonian Academy of Security Sciences and colleagues from the Estonian Tax and Customs Board and the Estonian Internal Security Service received training. Officials of the FIU gave presentations at a number of conferences, seminars, workshops, training activities and other events.

Table 3. Training activities organised by the FIU between 2017–2019

	2017	2018	2019
Number of training activities	14	16	20
Number of participants	588	841	1223

The FIU's partners include obliged entities, law enforcement agencies and supervisory authorities. The Estonian Banking Association is our good partner that helps to organise cooperation with banks. Both current issues and new trends are under discussion at the regular meetings of the Banking Association anti-money laundering task force. The exchange of information and cooperation with major reporting entities and many umbrella organisations and professional associations is also important.

Our cooperation partners in supervision are the Estonian Bar Association, the Chamber of Notaries and the Financial Supervisory Authority. Cooperation with the latter is particularly important in preventing money laundering, considering the importance of the financial sector in the anti-money laundering system. Therefore, the exchange of information with the Financial Supervisory Authority is particularly close.

The Financial Supervisory Authority's supervisory activities have had a considerable impact on market participants' actions and the FSA's activities over the past few years in the field of preventing money laundering have pushed the market situation in the right direction. The Ministry of Finance, the Ministry of the Interior and the Ministry of Foreign Affairs are valuable partners in the prevention of money laundering and terrorist financing, and shaping an effective legal environment for implementing international financial sanctions. By participating in the work of the AML/CFT Committee of the Ministry of Finance, we can contribute to the formulation of national policies and legislation on both the prevention of money laundering and terrorist financing.

National cooperation with all investigative bodies is working. If the FIU decides on the basis of its analysis that an incident may involve money laundering, terrorist financing or related crimes, it forwards its materials to other law enforcement agencies. In 2019, the Financial Intelligence Unit sent information to other law enforcement agencies on 420 occasions, of which more than a half were responses to inquiries and materials sent for informational purposes (Table 4). On 23 occasions, materials were sent to make a decision whether to commence criminal proceedings. As of 31.12.2019, investigative bodies commenced proceedings in 13 cases, including 10 cases of money laundering. On six occasions materials forwarded by the FIU were annexed to an ongoing criminal matter, on three occasions the proceedings were commenced under another section and on four occasions investigative bodies refused to commence criminal proceedings. Fraud was the prevalent presumed predicate offence among reports of criminal offence. The number of materials sent to be annexed to an ongoing criminal matter was 131.

Table 4. Materials forwarded to law enforcement bodies by the FIU between 2017–2019

	2017	2018	2019
Criminal complaints	14	52	23
... criminal proceedings commenced as of 31.12	13	36	13
... incl. money laundering proceedings commenced	8	26	10
To be annexed to an ongoing criminal matter	59	95	131
Responses to queries, sent queries, for information	169	204	266
Materials forwarded for investigation in total	242	351	420
Amounts relating to forwarded materials	79.1 million	1.77 billion	3.6 billion

190 criminal proceedings were commenced in Estonia on the grounds of money laundering in 2019. As mentioned above, 10 of these were commenced on the basis of the material sent by the FIU (Figure 6). The vast majority of them (90 criminal proceedings) were provided by two criminal cases in which individuals partially overlap and relate to computer fraud committed between 2015 and 2018.

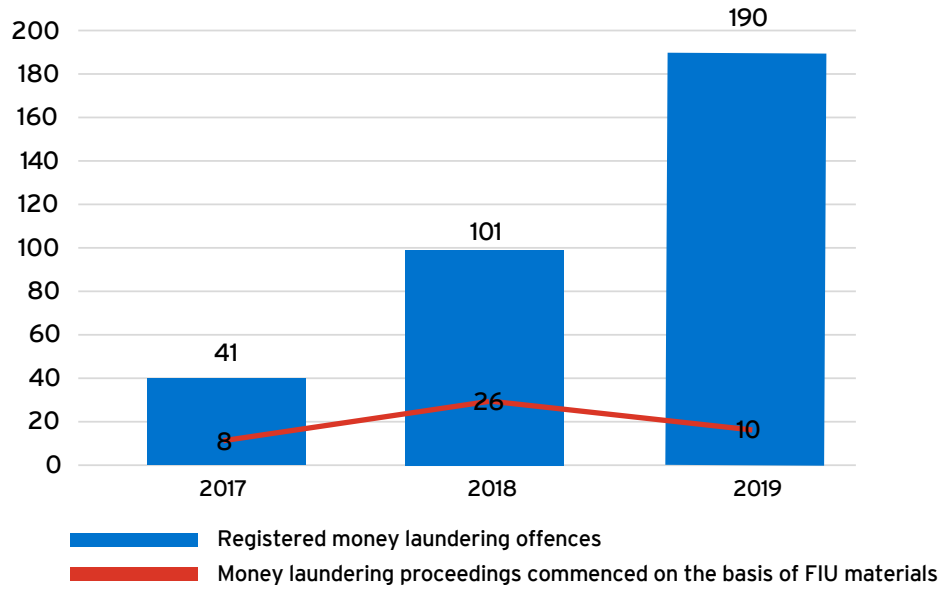


Figure 6. The number of money laundering offences registered in Estonia and the number of money laundering proceedings commenced on the basis of the materials forwarded to the investigative bodies by the FIU between 2017–2019

Note: information on the number of registered money laundering offences was obtained from the Ministry of Justice.

As in the previous two years, the materials submitted in 2019 mostly used the information contained in the reports sent by credit and financial institutions.

In recent years, significant developments have taken place in multilateral cooperation between the FIU, the investigative bodies, the Prosecutor's Office and the Financial Supervisory Authority. Bilateral relations between the FIU and its partners used to dominate the scene, but as the anti-money laundering and related proceedings have gained importance, the level of multilateral and coordinated cooperation is growing.

The most prominent cases of national cooperation have also been covered in the media: criminal proceedings commenced on suspicion of money laundering concerning the activities of GFC Good Finance Company AS and Swedbank AS. In addition, the FIU continued to contribute to the criminal proceedings concerning the Estonian branch of Danske Bank A/S. In addition, the FIU has been able to provide assistance to units dealing with criminal proceedings regarding the movement of defrauded money in Estonia and abroad gained from cyber scams.

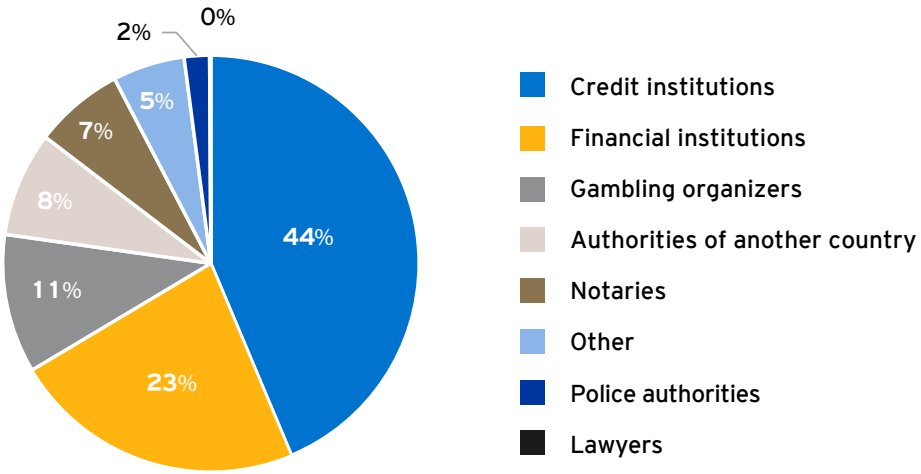


Figure 7. Distribution of reports received by the FIU used in forwarded materials based on the groups of senders in 2019

The FIU can contribute to the withholding of criminal proceeds if the possibility of seizure in criminal proceedings has expired in connection with the commission of a bankruptcy offence, as discussed previously in the yearbook. The seizure applied to the debtor's assets prior to the declaration of bankruptcy ends with the declaration of bankruptcy. If a company whose assets have been seized in criminal proceedings finishes its activities with a criminal bankruptcy during the proceedings, it is possible that criminal assets included in the assets of the company can no longer be seized in criminal proceedings. In such a case, the FIU restricts the disposal of the assets in order to preserve the victim's assets.

With regard to transactions suspected of terrorist financing, the FIU cooperates closely with the Estonian Internal Security Service (KAPO) by forwarding reports of suspected terrorist financing to KAPO and, if necessary, uses the assistance of its foreign partners to clarify the background of suspected assets and persons.

The FIU's analyses are mostly based on tracing money. It is necessary to obtain information about the origin of the money and its possible connection with the predicate offence. In order to monitor the flow of money, it is also often necessary to use the assistance of foreign authorities. Therefore, international cooperation is crucial for the FIU. The FIU can make inquiries to other FIUs in order to obtain additional information on suspicious transactions and, if necessary, restrict the disposal of assets abroad. Incoming information from abroad may help to identify foreign criminals exploiting the Estonian financial system and the FIU can share this informa-

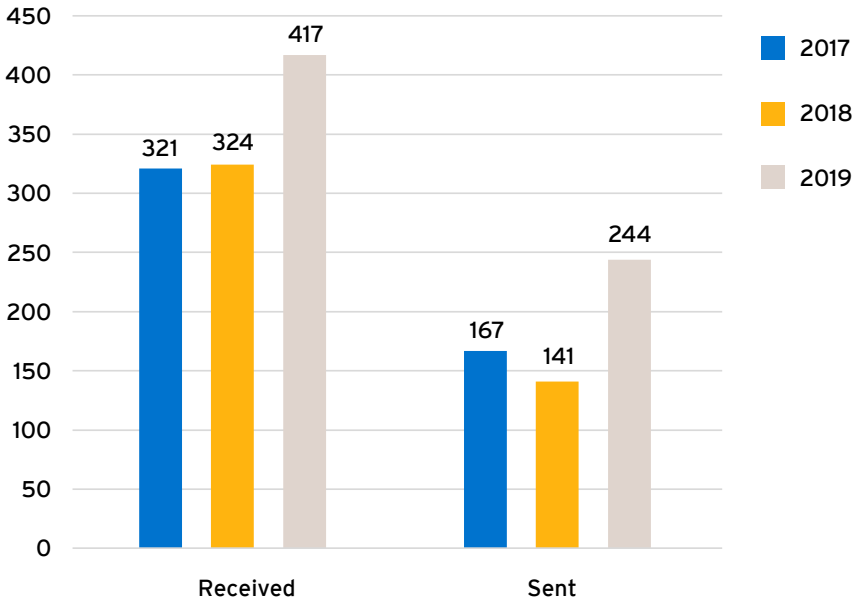


Figure 8. The number of foreign inquiries received and sent by the FIU between 2017–2019

tion with our law enforcement authorities. The FIU regularly takes part in the international meetings of the Egmont Group, in the Council of Europe's expert committee MONEYVAL and the European Union Financial Intelligence Units Platform called EU FIU Platform.

In 2019, the FIU received 417 inquiries from a total of 55 countries and sent 244 inquiries to 45 foreign countries (Figure 8). A foreign state provided information to the FIU on its own initiative on 117 occasions and on 24 occasions the FIU provided information to a foreign state on its own initiative. The large number of queries received illustrates the cross-border nature of money laundering offences and the fact that the FIU is contributing to the prevention of money laundering and terrorist financing not only locally but also on an international scale. The average time for responding to foreign queries in 2019 was 12 days.

As before, the closest cooperation in 2019 took place with neighbouring countries. Most foreign inquiries were received from the Latvian FIU (64), the Finnish FIU (38), the Lithuanian FIU (36) and the Russian FIU (32). Estonia sent most of its foreign inquiries to the Latvian FIU (28), the Russian FIU (24) and the UK FIU (21).

With our foreign colleagues, we exchange information on current urgent cases, where in addition to rapid sharing of information, partner institutions can be assisted in imposing temporary restrictions on disposal of property, as well as part of a more thorough financial investigation alongside criminal proceedings. There is operational cooperation between EU Member States via FIU.net, and through Egmont Secure Web we also exchange information with colleagues from third countries; the cases analysed are often still in the phase of seeking confirmation of a suspected money laundering.

When it comes to external cooperation, the contribution of the FIU to important criminal cases in other countries is worth mentioning. A couple of major cases of cooperation with the Russian Federation and Ukraine, as well as with the United Kingdom and Latvia, should be highlighted. While we have provided input to Latvia in a wide range of criminal investigations into tax fraud, we cooperated with the UK on a large-scale transit cash flow that passed through Estonia in 2010-2015, which may be related to corruption in a CIS country.

The flow of criminal money from Russia over the last decade through Estonia's financial system has also been a subject of the current cooperation. In 2019, we received many inquiries from Ukraine in connection with the laundering of corrupt income through the Estonian financial system between 2013 and 2018. The amounts in these cases vary to a large extent: from a couple of millions to tens of millions of euros. Such criminal cases in Ukraine are potential predicate offences for money laundering proceedings in Estonia.

Another example of good cooperation with Ukraine is the case covered in the OCCRP, in which the FIU imposed a restriction on the disposal of 500,000 euros. The money came from a former Ukrainian politician and attempts were made to integrate it into the economy through the Estonian financial system by purchasing a racehorse from Germany.

In addition to the aforementioned countries, Lithuania, Malta, Finland and the United States were the most active cooperation partners in 2019. Belarus also became very active at the end of 2019, so in 2020 Belarus can be expected to make as thorough inquiries in criminal cases as those from Ukraine and Russia.

We have received a large number of inquiries from different countries about fraud, where the money from a criminal offence has been transferred to an account in an Estonian credit institution held by a payment intermediary registered in the UK, and has then immediately been converted into a virtual currency. Foreign authorities have also made inquiries about Estonian companies in connection with fraudulent investment platforms. In these cases, it is difficult for us to help our foreign partners, as the level of contact with Estonia is minimal: foreigners or Estonian e-residents are behind the companies registered in Estonia and, in addition, these companies do not have bank accounts in Estonia. In general, it is also the foreign nationals who have fallen victim to these cases. The number of inquiries concerning various crowdfunding platforms has also increased.

Banks' stricter anti-money laundering policies can also be seen in the analysis of foreign inquiries. In particular, the accounts of many Estonian non-residents, about which foreign colleagues request information in their foreign inquiries, have already been closed in Estonian banks, and the banks have also notified the FIU of such former customers. Another trend we are seeing is that the Estonian companies the FIU receives foreign inquiries about, do not have bank accounts in Estonia, but have opened accounts in another European country.

2.3. SUPERVISION

The FIU has a statutory function of performing state supervision over certain market participants. These functions are imposed on the FIU by the Money Laundering and Terrorist Financing Prevention Act and the International Sanctions Act. In 2019, the FIU conducted 20 on-site inspections and 36 remote inspections (Figure 9). Misdemeanour proceedings were commenced on eight occasions, the most common violation being shortcomings in the due diligence obligations.

A more detailed overview on supervisory activities can be found in Table 5.

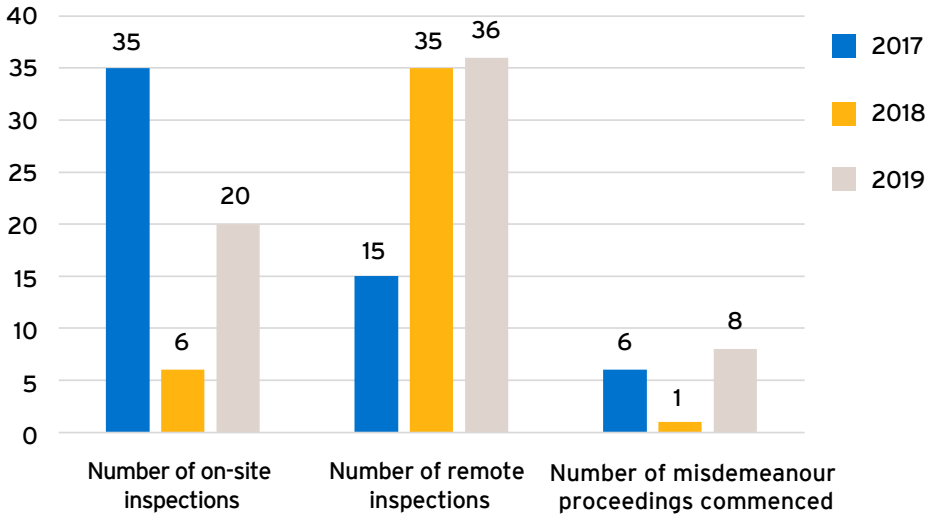


Figure 9. Supervisory inspections and misdemeanour proceedings between 2017–2019

In 2019, the supervisory activities of the FIU could be mainly divided into two main areas of work: supervisory activities in the virtual currency sector (providers of the service of exchanging virtual currency against a fiat currency and providers of virtual currency wallet service) and inspections of real estate brokerage companies.

Table 5. Distribution of inspections carried out by the FIU in 2019, based on the business activities of the persons inspected

Field of activity	Number of inspections
Credit institution	1
Financial institution	11
Trader	1
Real estate broker	8
Trust and company service providers	1
Providers of a service of exchanging a virtual currency against a fiat currency	2
Providers of a service of exchanging a virtual currency against a fiat currency and virtual currency wallet service	32
TOTAL	56

The virtual currency sector is characterised by a lack of transparency in transactions, as the sector has not imposed a reporting obligation for data characterising the provision of services. The owners and members of the management boards of most service providers who have applied for an authorisation in Estonia are foreign nationals, so it has not been possible to carry out on-site inspections as the companies simply do not have a real office in Estonia and do not keep any documents related to the provision of the service. Therefore, in most cases, remote inspection had to be used to conduct national supervision proceedings in this sector. In a number of cases, the FIU had also received negative information about the companies, such as suspicions of fraud in relation to customers, or other financial services were provided abroad without proper authorisation. The FIU has repeatedly highlighted the risks associated with virtual currencies. The risks associated with the activities of

service providers are higher and the sector needs to be paid the highest possible attention through supervision proceedings.

In the course of the supervision procedures, it was established (on 31 occasions out of 34 proceedings conducted) that the companies had not started providing the service in Estonia and, as a result of the proceedings, the FIU revoked the authorisations of 31 companies.

Providers of property ownership or right of use transactions were also at the forefront of supervision in 2019. Inspections were carried out on all major real estate brokerage companies, a total of eight companies. At the beginning of the supervision proceedings, there was a noticeable activation of the sector. Umbrella organisations (Estonian Chamber of Estate Agents, Association of Estonian Real Estate Agents) approached the FIU with their requests for both organising training and preparing guidance material. The FIU contributed to the organisation of trainings as well as provided input to guidance materials. As a result of the inspections, a number of shortcomings were found in the performance of market participants both in the application of due diligence measures and in compliance with the obligation to record data, so the FIU is planning to continue inspecting market participants in this sector in 2020.

2.4. GRANTING OF AUTHORISATIONS

The number of applicants for authorisations has increased considerably in recent years. While in 2018 the FIU had to process 1430 authorisation applications and the increase compared to 2017 (108 applications) was almost 14 times, in 2019 the FIU processed 1690 authorisation applications. Since the FIU is also required to carry out proceedings for the revocation, suspension and amendment of authorisations (there were 128 revocations and 493 amendments in 2019), 2019 can be characterised as a highly demanding and labour intensive year in the field of authorisation-related proceedings.

Most applications for authorisation continue to be related to the development of new technologies and related services for the transfer or storage of value in digital form, i.e. the exchange of virtual currencies against a fiat currency and the provision of virtual currency wallet service. As a trend, authorisations for the provision of these services continue to be applied for together, as was the case in 2018, i.e. an authorisation is applied for both for the exchange of virtual currencies against a fiat currency and for the provision of wallet services. In most cases, this is done by companies whose members of the management body or actual beneficiaries are foreigners. According to the FIU, the risks of money laundering and terrorist financing in the sector are high and

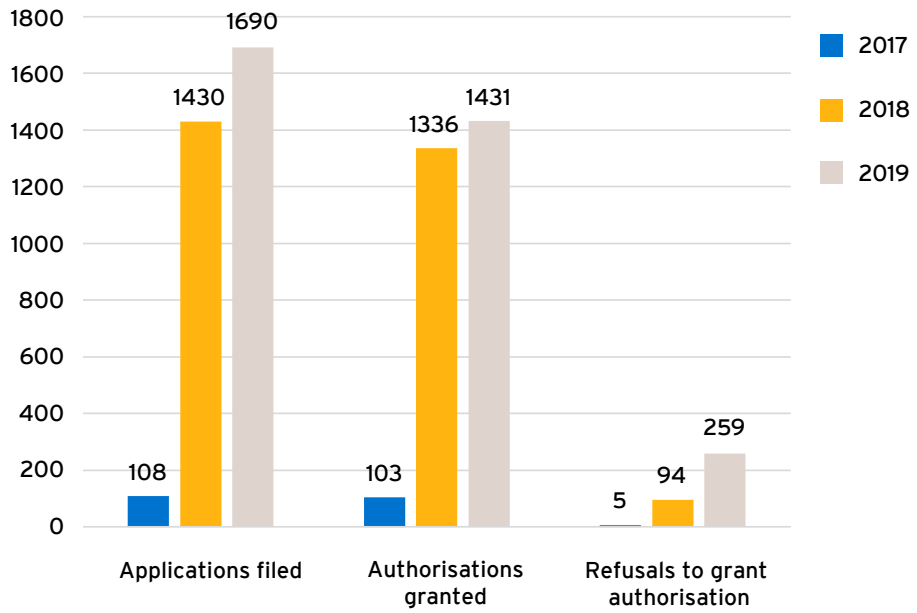


Figure 10. Overview of the applications for authorisations in 2017–2019

the threshold for obtaining an authorisation (requirements set by the circumstances of the object of inspection) is too low to prevent riskier companies from entering the market and to mitigate the risks associated with virtual currency service providers. Therefore, in 2019 the FIU also contributed to the legislation on the application for authorisations and the legislator decided to introduce additional and stricter requirements for access to the market for these services, as presented in section 1 of the yearbook.

In 2019, the FIU received 1690 applications for authorisation, of which 1431 were granted. (Figure 10).

The largest number of applications for authorisation submitted to the FIU were related to the provision of virtual currency services (Table 6).

Table 6. Distribution of applications for authorisation submitted to the FIU in 2019, based on the business activities of the applicants

Field of activity	No of applications submitted	No of authorisations granted
Financial institution	91	57
Pawnbroker	6	5
A service of exchanging a virtual currency against a fiat currency	775	667
A virtual currency wallet service	744	638
Dealing with precious metals	9	7
Trust and company service	65	57
TOTAL	1690	1431

3. COURT DECISIONS ON MONEY LAUNDERING CASES IN 2019

3.1. CRIMINAL PROCEEDINGS

Nine court decisions on money laundering entered into force in Estonia in 2019. Two persons, including one individual and one legal person, who had been suspected of money laundering were acquitted in 2019 because the prosecutor withdrew charges. 13 persons, including 12 individuals and one legal person, were convicted of money laundering. In three cases, the predicate offence of money laundering was computer fraud, in two cases it was fraud, in two cases a tax fraud and, in one case, accepting a bribe. The text of one judicial decision has not yet been published by the court due to another pending judicial procedure.

In 2019, property was confiscated from seven convicts of money laundering. A total of approximately 470,000 euros, as well as other assets (real estate, vehicles, computers), were seized.

Violation of public procurement requirements, bribery and money laundering

In May 2019, X was convicted under settlement proceedings of a particularly serious violation of public procurement requirements, accepting and requesting a bribe, large-scale money laundering, falsification of documents and the use of falsified documents.

At the time of the commission of the crimes, X worked as a technical director of the infrastructure engineering service in a hospital in Estonia. The hospital appointed X as a member of the Public Procurement Committee in the field of infrastructure, where he was responsible for participating in the preparation of procurement documents, the work of the Tender Evaluation Committee and the selection of a successful tenderer for public procurements.

During the preparation of the procurements, X coordinated and adjusted the terms of several hospital procurements with the representatives of companies OÜ A, OÜ B, AS C, AS D and OÜ D in such a way that these companies would be able to participate in the procurements and their tender would be successful. X preferred these companies in the procurements because the representatives of several of them gave bribes to him between 2012 and 2016.

In doing so, X infringed the requirements of the Public Procurement Act, including the general principles of public procurement – transparency, equal treatment and effective use of the existing competitive conditions – and the procurement procedures established in the hospital and gave those companies an advantage in participating in the procurement.

In order to obtain a bribe, X issued invoices totalling 105,333 euros to those companies on behalf of his related companies. X took out the money in the form of dividends, which he paid to himself and to his relatives.

The court sentenced X to 1 year and 8 months' imprisonment for the breach of public procurement requirements, 2 years and 6 months' imprisonment for accepting bribery and 2 years and three months' imprisonment for money laundering. All of them were conditional discharges, i.e. imprisonment would not be enforced if the accused did not commit another intentional crime during the 3-year and 8-day probation period.

92,048 euros, a car worth about 23,000 euros and nine gold coins worth 10,533 euros were confiscated from X.

Tax fraud and money laundering in Finland

X was convicted under settlement proceedings of helping A and B in Estonia with laundering money received as a result of tax offences committed in Finland in the total amount of 65,435 euros between August 2012 and September 2014.

The complicity consisted of X providing his bank account details and enabling A and B to transfer to it the proceeds of tax fraud and accounting offences in Finland on the basis of fictitious transactions. The receipts were intended to give the impression that X had received them as remuneration.

X was sentenced to 1 year and 10 months' suspended imprisonment for aiding money laundering and a car, a snowmobile, a van and a boat trailer were confiscated from him.

In another case, Y and Z were convicted under settlement proceedings of helping to conceal tax fraud and accounting offences committed by the responsible persons of five companies in Finland between May 2010 and September 2014, resulting in funds totalling 4,273,272 euros. To this end, Y together with LV set up a criminal organisation of four persons with the aim of committing money laundering. The criminal organisation was active until September 2014 and included, in addition to Y and LV, JN from January 2011 and EV from March 2012. The latter two contributed to the achievement of the objectives of the group led by Y and LV and fulfilled the roles defined in accordance with the instructions given by Y and LV in the criminal organisation.

Y's role in the criminal organisation was to organise its activities between January 2011 and September 2014. He set it up, led the organisation and recruited JN and EV as its members.

The task of Y was to set up or find companies to which LV could transfer funds from A OY's accounts received as a result of tax fraud and accounting offences and to find board members for those companies who would be willing to withdraw cash transferred from A OY's accounts to the bank accounts of the companies created so that the money could be returned to LV.

In accordance with the established scheme, Y gave orders, tasks and instructions to JN and EV, the members of the criminal organisation, for money laundering, as well as for the distribution of the wealth gained. In the interests of the criminal organisation and in order to ensure the stability of the organisation, Y also recruited various persons for the purpose of cash withdrawal from financial institutions based in Estonia of funds obtained as a result of crimes committed in Finland. Under his instructions, these persons set up new companies and, in order not to arouse any suspicion, withdrew the cash received as a result of tax offences committed on behalf of different companies during different periods of time, with a view to return it to LV through Y. According to the agreement with LV, Y received 4%–6% of the amounts transferred from Finland and withdrawn as cash in Estonia for organising cash withdrawals, preparing the underlying fictitious invoices and returning the money to LV.

In total, the criminal organisation led by Y and LV carried out financial activities amounting to a total of 8,824,827 euros, which was mixed with funds from non-criminal sources, but included funds received as a result of tax fraud and accounting offences committed by the responsible persons from different companies in the Republic of Finland, which were in turn mixed with each other, amounting to a total of 4,273,272 euros.

Z was accused of giving Y his bank account details and allowing Y and JN, on the basis of fictitious transactions, to transfer him money obtained through tax fraud and accounting offences totalling 91,020 euros. The amounts received were intended to give the impression that they were remuneration (the scheme is similar to that of X). In practice, Z (or X) was not employed in the companies, and the transfers concerned fictitious transactions which decoupled funds from tax fraud and accounting offences committed in the Republic of Finland and concealed the true origin and ownership of those funds, thus legalising the funds obtained by committing the offences through the ostensible payment of legal remuneration.

Y was sentenced to 5 years' suspended imprisonment for organising a criminal group and 4 years' suspended imprisonment for money laundering. 830 euros in cash, 2 properties, a tablet and a laptop were seized from Y, in addition to 70,600 euros to replace the seizure.

The court sentenced Z to 2 years' suspended imprisonment for aiding money laundering and confiscated 4,268 euros from Z.

3.2. ADMINISTRATIVE COURT PROCEEDINGS

In 2019, the only administrative case initiated in 2018 came to an end. The case was also discussed in the previous yearbook of the Financial Intelligence Unit. The administrative court ruled in the matter, confirming that the refusal of the FIU to grant authorisation was in accordance with the law.

Restrictions on disposal imposed by the FIU were brought before the courts on four occasions in 2019. One of them was resolved in an administrative court in favour of the FIU, while three complaints are pending as of the beginning of 2020. In two of the three complaints referred to, an application for interim relief was also made, in which one was awaiting acceptance/rejection by the Supreme Court in 2019, while the other was rejected by an administrative court.

In 2019, two restrictions of up to one year were imposed, both of which were appealed to the district court, which in both cases upheld the restriction. In one case, the decision of the circuit court was appealed to the Supreme Court, which could not decide whether to accept or reject it within the last year.

4. MONEY LAUNDERING SCHEMES

Below, we provide an overview of the schemes analysed by the Financial Intelligence Unit in 2019.

Cyber fraud

Investment fraud has aroused a strong reaction. The basic scheme of it can be summarised as follows: people are invited to invest, but in reality, fraudsters do not have any plans to provide investment services and investors lose their money. A variety of financial institutions are used, which may have an authorisation, but not for the provision of investment services. In the online environment, pages are created that allow you to choose an investment object, transfer money and wait for your return. However, the investment cannot be converted back to cash. Various legal forms are used to perpetrate such fraud – a private limited liability company with an authorisation of a financial service provider and/or a provider of a service for exchanging a virtual currency against a fiat currency, a crowdfunding platform operator, a savings and loan association, etc. Both fiat currency and virtual currencies can be used to commit fraud.

The various stories used to make people loosen their purse strings can sometimes be classified as fiction as they seem so unrealistic. Whoever follows the various forums on the Internet will see the schemes put forward by the victims.

The FIU identified the following as one of the most recent schemes:

The perpetrators of the fraud claim that they have a company that has directed its activities towards investment as well as precious metals, solar energy, etc. (it offers titanium plates that are supposed to be of very high market value and make people rich), therefore the company has a bank account at Mack Gold and is a major customer of the bank. The fraudsters claim that the bank wants to make a gift to them as a major customer: the customer can buy luxury cars by paying only 40% of their price, and the remaining 60% is paid by the bank on behalf of the customer. Allegedly, the company itself does not need these cars and therefore offers them to people who might be interested. The only requirement is that the person chooses the car in their home country and pays 40% of the invoiced amount to a bank account abroad (United Arab Emirates). The bank would then pay 60% of the price to the car dealer, after which the person can pick up the car at a showroom. Another condition is that the person must pay a membership fee of 200 euros in order to become a member of the company, as the offer applies only to the people of their company.

It is very often a common feature of fraud in cyberspace that, in order to receive a good, service or gift, a person has to contribute to some extent. For the first time, the payment is usually not high and it is not considered to be much to be paid for the expected potential benefit. In most cases, however, people receive nothing but new demands. If the value of the goods and/or services to be purchased does not correspond to the deposit, in

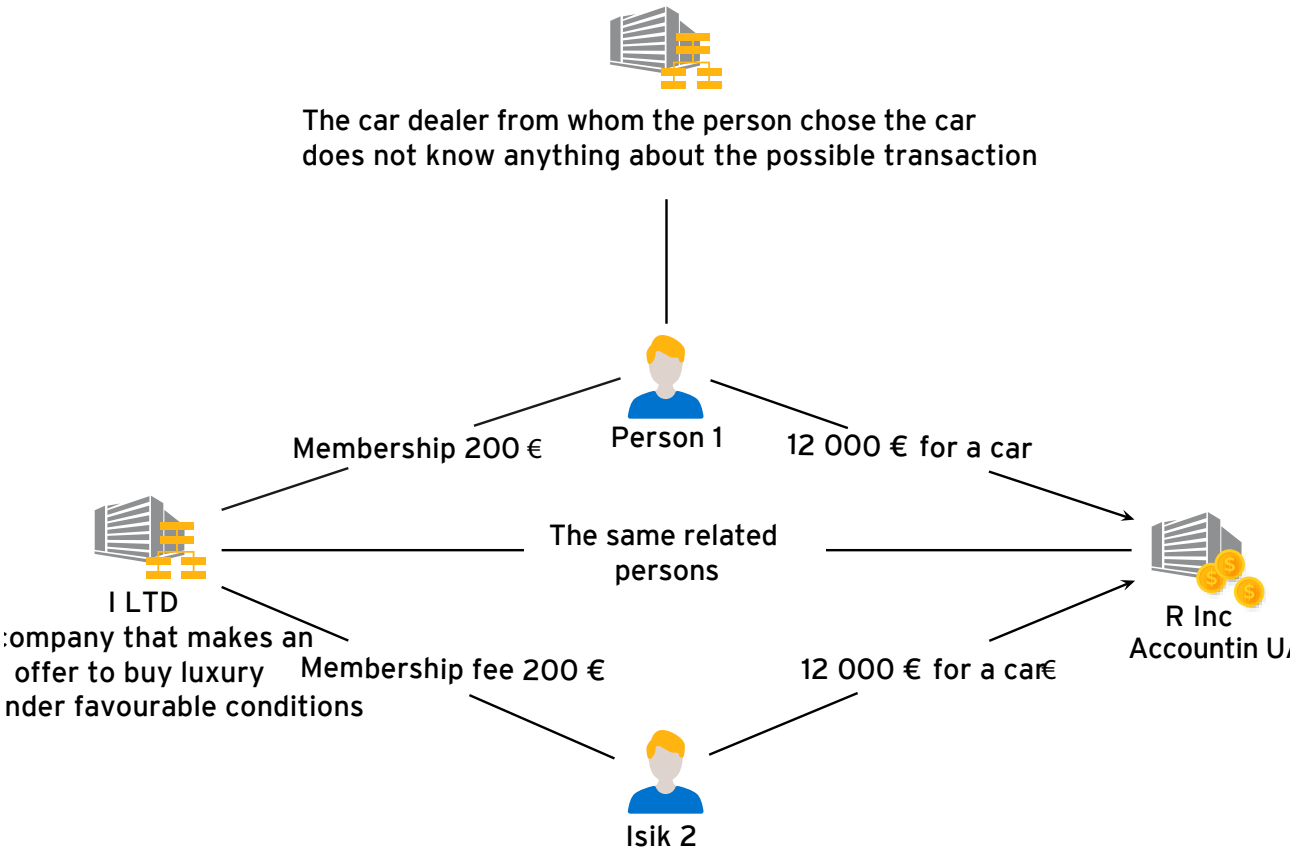


Figure 11. Luxury cars fraud

most cases you will be dealing with fraud. Therefore, especially in the case of online transactions, it is necessary to maintain common sense and to think twice whether the offer is in line with reality.

In the case of cyber fraud, it is possible not only to fall victim but also to become an accessory to it. It happens when a person allows money of unknown origin, which may have been obtained as a result of fraud, to be transferred to their account. A small fee is charged, the rest is withdrawn or transferred to third parties. Such a person is known as a money mule and may also be punished as an accessory to a criminal offence. Everyone should be careful not to be used to move criminal money or commit crimes such as terrorist financing. This risk is very real without knowing the origin of the money or to whom the money will be transferred.

Laundering money received from a predicate offence related to a foreign state-owned enterprise in the Estonian financial system

In many cases, criminals make use of the opportunity to move proceeds of crime abroad and use the financial systems of other countries to launder it. Managers are able to cause significant damage to public companies with a complex structure and management culture by acquiring the assets of the companies they manage or by gaining competitive advantages through corrupt practices. The proceeds of crime are taken out of the country by using partners, with whom cooperation has worked in the past.

This scheme refers to the transfer of criminal proceeds obtained as a result of misappropriation of funds from various state organisations and companies and corruption from Russia, Belarus and Ukraine to the Estonian financial system for the purpose of money laundering. In most cases, the money is not intended to remain in Estonia permanently, but moves forward. Most crimes have been committed a few years earlier.

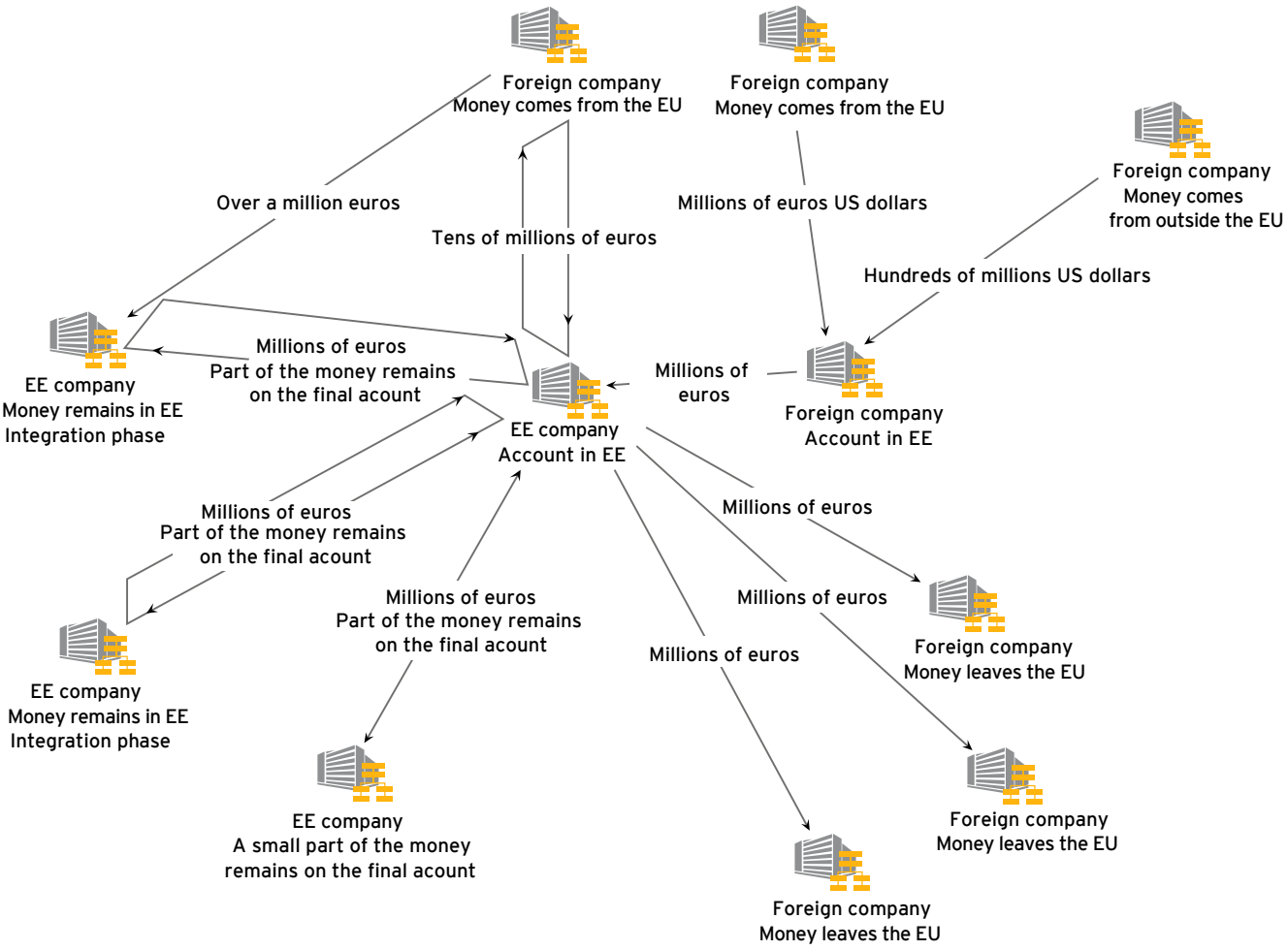


Figure 12. Estonian companies and bank accounts in an international money laundering scheme

Insolvency offences

Two Estonian companies received money in their accounts through criminal activities (obtaining financial gain through illegal interference in the data processing procedure). The companies were linked to each other through joint ownership. In order not to lose the assets, one company initiated bankruptcy proceedings against the other. Fictitious claims were included in the bankruptcy proceedings. Such activities created a money laundering process, which sought to conceal the origin of the proceeds of its illegal activities and to regain control of the assets to be laundered by creating fictitious claims and a state compatible with bankruptcy.

In this way, the individuals tried to escape seizures applied in criminal proceedings. According to section 45 of the Bankruptcy Act, seizure applied with regard to the debtor's assets before the declaration of bankruptcy terminates with the declaration of bankruptcy. Therefore, the seizure of the assets was terminated, but the persons who initiated the bankruptcy proceedings failed to take control of the assets, as the Financial Intelligence Unit identified such an activity and applied a restriction on their disposal. The Prosecutor's Office initiated a new criminal investigation based on the criminal report filed by the FIU. The case was investigated by the Criminal Bureau of the North Prefecture. By the time of publication of this yearbook, the court has ruled. The perpetrator was found guilty of money laundering and the victim's assets were excluded from the bankruptcy estate. By now, the assets have been returned to the victim.

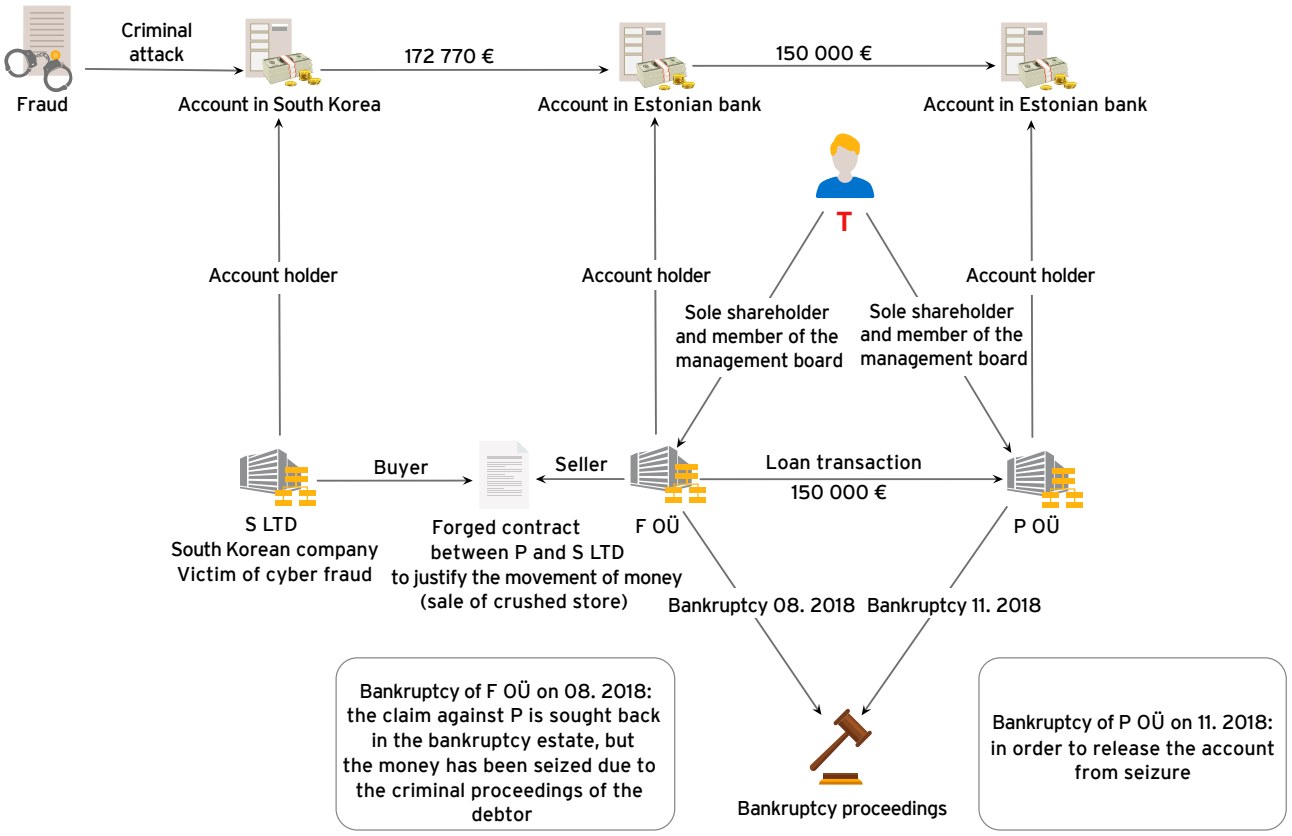


Figure 13. Exploitation of bankruptcy proceedings

Sale of shareholdings

In 2019, there were several cases where the holdings of Estonian private limited companies were sold at a price significantly higher than their expected value. In a number of cases, such an increase in value was not justified either in the company's annual reports or on the basis of the company's activities. The buyers of the shares were often foreign legal or natural persons who could not justify the origin of the assets used to finance the transaction or, in some cases, the reasons why they were willing to acquire a foreign company at a price higher than its value. Although transactions take place in Estonia, there were cases where the money for the company's shares was either moved outside the Estonian financial system, originated from abroad or was paid in cryptocurrency. If assets come from abroad, their origin is more difficult to trace and the risk of illegally acquired assets entering our financial system is high.

Selling company shareholdings at a higher price, unless economically justified, provides criminals a good opportunity to direct their assets of unclear origin to seemingly active companies.

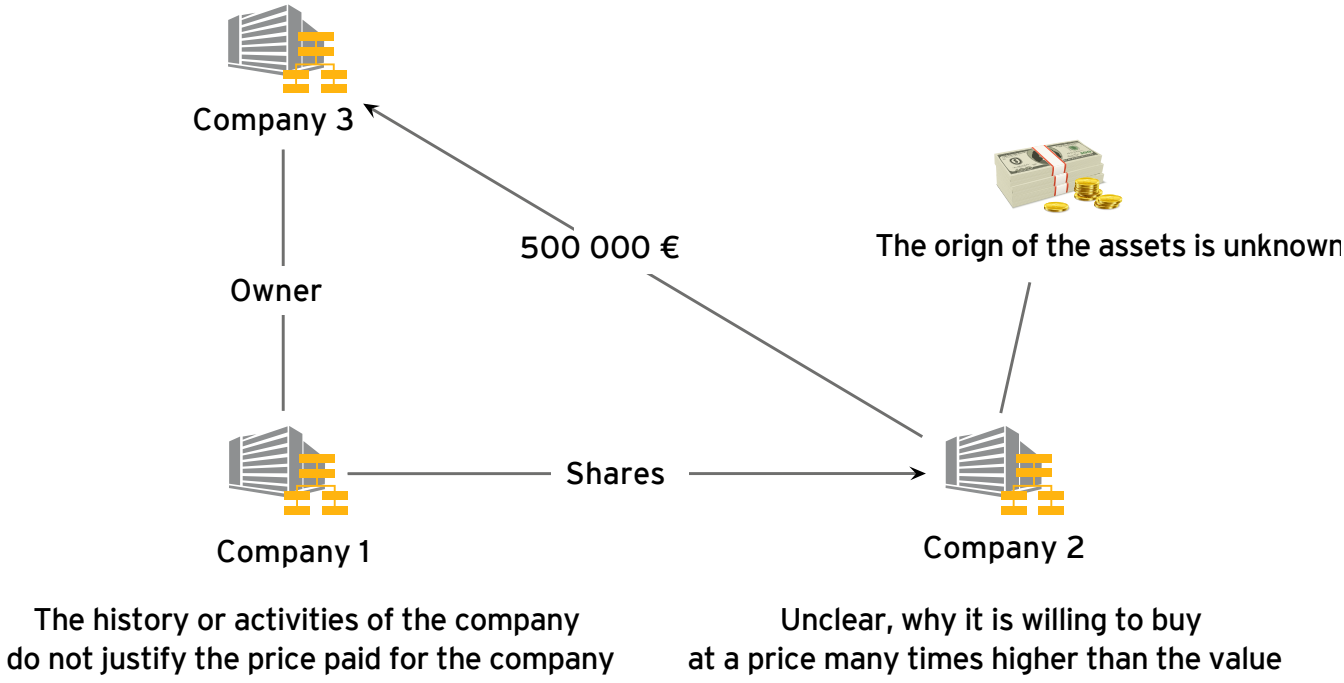


Figure 14. Money laundering through the sale of shares

5. INTERNATIONAL FINANCIAL SANCTIONS

2019 was a busy year for the FIU regarding the performance of tasks related to the implementation of international financial sanctions. There were a number of cases in which sanctions had to be imposed. Out of those, the case of Rossiya Segodnya (Russia Today) received increased public attention. The tasks of the FIU related to the application of financial sanctions can be conditionally divided into two: firstly, state supervision over the implementation of financial sanctions with regard to compliance with the requirements of the International Sanctions Act, and secondly, verification of the legality of the measures taken by market participants in the implementation of the sanction following the corresponding notification.

Pursuant to subsection 16 (2) of the International Sanctions Act, the FIU shall publish, once a year, a consolidated overview of the implementation of financial sanctions concerning the identified subjects of financial sanctions, financial sanctions applied and the exemptions made or authorisations granted. This information is presented in Table 7.

Table 7. Implementation of financial sanctions in 2019

No	Date	Subject	Sanctions applied	Exemption/ Authorisation
1	16.07.2019	A. Rotenberg / Agricultural Minerals DMCC	Unavailability (67,800.00 EUR)	No
2	21.10.2019	Dmitry Kiselyov / MIA Rossiya Segodnya (Russia Today)	Freezing (1000.00 EUR)	No
3	22.10.2019	Dmitry Kiselyov / MIA Rossiya Segodnya (Russia Today)	Freezing (2879.42 EUR)	No
4	08.11.2019	Dmitry Kiselyov / MIA Rossiya Segodnya (Russia Today)	Freezing (30,005.08 EUR)	Yes
5	25.11.2019	Dmitry Kiselyov / MIA Rossiya Segodnya (Russia Today)	Freezing (30,005.08 EUR)	Yes*
6	09.12.2019	Dmitry Kiselyov / MIA Rossiya Segodnya (Russia Today)	Freezing (31,848.41 EUR)	Yes*
7	30.12.2019	Dmitry Kiselyov / MIA Rossiya Segodnya (Russia Today)	Freezing (89,577.00 EUR)	Yes*

* The exemption was granted in 2020.

The FIU had two major cases related to the application of international financial sanctions in 2019 – MIA Rossiya Segodnya and OOO Minudobreniya. Both are based on the activities of enterprises linked to persons sanctioned under the sanction regime established by the Council Regulation (EU) No 269/2014.

The first major case, which also found widespread media coverage, concerned the implementation of financial sanctions against MIA Rossiya Segodnya and Dmitry Kiselyov. This is a relatively old case, which the FIU reflected in its 2015 yearbook. Dmitry Kiselyov was included in the EU's sanctions lists in 2014 for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. Dmitry Kiselyov's sanctions extend to the legal entities under his control, including MIA Rossiya Segodnya, a company wholly owned by the Russian Federation.

MIA Rossiya Segodnya opened a current account with a credit institution in Estonia. After ascertaining that the company was controlled by Dmitry Kiselyov, the bank imposed financial sanctions on the company by freezing its assets. The freezing of the current account is also in force at the time of completion of the yearbook. As a follow-up to this case, other Estonian credit institutions identified payments made by or with the participation of MIA Rossiya Segodnya between October and December 2019 and also started to actively implement restrictive measures.

After the restrictions, the dissemination of misinformation showed the application of sanctions as a restriction of the freedom of the press in Estonia. The application of sanctions is not related to the field of activity of Rossiya Segodnya and sanctions are applied irrespective of the activity of the sanctioned person.

MIA Rossija Segodnya filed a petition to court against Estonian FIU, challenged the activities of the FIU and the legitimacy of imposing EU sanctions on Rossija Segodnya. We are awaiting a court ruling, including the court's position on the implementation of EU financial sanctions. Follow-up activities to this case continue into 2020.

The second major case in 2019 was the so-called fertiliser case, i.e. the adoption of restrictive measures in relation to the activities of AO Minudobreniya. The case concerns a fertiliser production plant (so-called ROSSOSH) in the Russian Federation, the products of which have been purchased by many Estonian farms and is operated by a company called AO Minudobreniya. The production is resold to Estonian farmers, usually in the form of seasonal fertiliser sales before spring and autumn sowing. According to public articles, the fertiliser plant is owned, through various holdings in Cypriot companies, by Arkady Rotenberg, who is included in the EU sanctions lists for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. The sale of fertiliser from Russia to Estonia was organised through a front company called Agricultural Minerals DMCC (a company in the United Arab Emirates which used a bank account opened in Germany) for which the connection with the sale of fertiliser could also be identified through articles published in the public press. The bank identified the situation with regard to the application of a sanction and refused to make payments. The FIU informed other credit institutions as well as other potential customers of the company about the need to impose sanctions.

6. LOOKING AHEAD TO 2020

In 2020, a number of important developments are expected in the Estonian money laundering and terrorist financing system.

In our view it is a significant risk that, against the backdrop of the reorganisation of the financial system in recent years, questions have begun to emerge as to whether our anti-money laundering system really needs to be made more effective, and whether perhaps the measures to combat money laundering need to be relaxed instead. These kinds of choices become particularly relevant in the light of the economic difficulties caused by the outbreak of the tragic coronavirus that hit the world at the beginning of the year. In this context, it is not superfluous to recall that the prevention of money laundering is not a one-off exercise and that the risks of money laundering and terrorist financing still linger. A number of shortcomings hampering the effective functioning of the anti-money laundering system, from the regulation of administrative penalties to the definition of the task of monitoring cash flows entering the country, remain to be addressed.

It is essential that the country's AML/CFT risk assessment carried out under the direction of the Ministry of Finance provides a comprehensive and adequate reflection of our risks and allows all actors in the system to shape their actions to mitigate these risks.

In the field of financial crime, a number of frauds in the area of crowdfunding came to light at the beginning of 2020. The number of cases of fraud involving virtual currency service providers and cases involving money laundering and terrorist financing risks show no signs of decline. The initial changes to the requirements for virtual currency providers, which entered into force on 10 March, will allow some unsuitable market participants to be removed from the market. However, they are far from sufficient to clean up the sector. In addition to the introduction of anti-money laundering requirements, it is high time to engage in substantive regulation in this area, bearing in mind the interests of consumers and the need to prevent fraud and abuse. The Ministry of Finance has started to better regulate the field of virtual currencies. We hope that this initiative will be delivered already in 2020.

The Financial Intelligence Unit is looking forward to the completion of the IT solutions for the so-called bank account registry in the autumn of 2020 so that banks can transmit data on bank account holders and suspicious transactions quickly in a modern way and in a standardised and machine-processable form. We hope this development to become a major step forward in the speed of information transmission and we will see related opportunities to better understand and highlight the risks of money laundering in our financial system.