

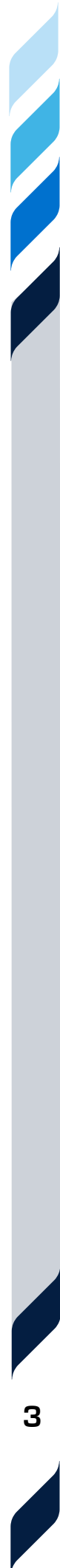
ESTONIAN FIU



YEARBOOK 2020



OVERVIEW OF THE ACTIVITIES OF THE ESTONIAN FINANCIAL INTELLIGENCE UNIT IN 2020



CONTENTS

PREFACE	4
1. YEAR 2020 IN ESTONIA'S ANTI-MONEY LAUNDERING SYSTEM	5
1.1. National anti-money laundering risk assessment	5
1.2. Changes in the legislation	5
1.3. Feedback for the reporting entities	8
1.4. IT developments in the Financial Intelligence Unit	9
1.5. Preventing the exploitation of crowdfunding platforms	9
1.6. Analysis of the ex-post reports submitted by the Estonian branch of Danske Bank A/S	10
1.7. The Financial Intelligence Unit participation in the Egmont Group project	10
2. A REVIEW OF THE FINANCIAL INTELLIGENCE UNIT'S WORK RESULTS IN 2020	11
2.1. A review of the reports received by the FIU and their analysis	11
2.2. National cooperation	16
2.3. International cooperation	19
2.4. Supervision	22
2.5. Granting of authorisations	23
3. COURT DECISIONS RELATED TO MONEY LAUNDERING IN 2020	25
3.1. Criminal proceedings	25
3.2. Administrative court proceedings	27
4. MONEY LAUNDERING SCHEMES	30
5. INTERNATIONAL FINANCIAL SANCTIONS	35
6. LOOKING AHEAD TO 2021	38



Dear Reader of the Estonian Financial Intelligence Unit Yearbook!

2020 was a challenging year for the Estonian Financial Intelligence Unit – the challenges included working from home during the Covid-19 pandemic, and taking the first steps necessary for establishing a new agency. Namely, the Government of the Republic decided that, as of 1 January 2021, the Financial Intelligence Unit would become an independent institution within the jurisdiction of the Ministry of Finance.

Year 2020 was the deadline to harmonise the EU's 5th and 6th Anti Money Laundering Directives into the member states laws and had to be incorporated into Estonian law as well. It also meant amending the Money Laundering and Terrorist Financing Prevention Act in Estonia in order to introduce the necessary changes to comply with the directives. We will also discuss these changes in our yearbook.

In 2020, Estonia continued to prepare its national risk assessment, in which the employees of the Financial Intelligence Unit also played a key role by participating in the work of the steering group and all working groups as well as by leading two of the working groups. The purpose of the national risk assessment was to identify threats, vulnerabilities and risks related to money laundering, terrorist financing and the financing of weapons of mass destruction in Estonia. Today, the national risk assessment has been completed and was published on the website of the Ministry of Finance in May 2021.

The impact of Covid-19 also caused the Financial Intelligence Unit to reduce its direct contacts, and therefore, less training was provided to obliged entities and fewer on-site inspections were made. However, for the first time, we provided written feedback to obliged entities. Feedback reports were sent to the eight largest reporting entities, as well as all obliged entity sectors that submitted reports. Sector-based feedback is available on our website.

In 2020, the number of reports received by the Financial Intelligence Unit increased. To a large extent, this was related to Danske Bank's obligation to provide information related to the follow-up analysis of its activities, as well as the fact that the digitalisation trend caused the pandemic enabled swindlers to operate more actively. There was also an increase in the number of reports from virtual currency service providers. The submission of more reports by obliged entities also increased the FIU's cooperation with law enforcement agencies in order to provide them with as much information as possible.

In order to reduce manual data processing, the development of the FIU information system also continued. All in order to better collect and analyse the information received by the FIU, and thereby, help to prevent money laundering and terrorist financing more effectively.

You'll find all this and much more in our yearbook.

Enjoy reading!

Margret Lundava, Acting Director, Financial Intelligence Unit



1. YEAR 2020 IN ESTONIA'S ANTI-MONEY LAUNDERING SYSTEM

1.1. National anti-money laundering risk assessment

In 2020, the compilation of a national anti-money laundering risk assessment (NRA), coordinated by the Ministry of Finance, was launched in Estonia. The purpose of the NRA was to get an overview of the threats, vulnerabilities and risks related to money laundering, terrorist financing and the proliferation of weapons of mass destruction in Estonia. This was the second time that a NRA was prepared in Estonia, the first Estonian NRA was completed in 2015.

This time, the NRA was based on PriceWaterhouseCoopers' risk assessment methodology, which was developed especially for the Estonian NRA. The NRA includes the years from 2017 to 2019. There was a total of nine working groups in the NRA, two of which, i.e., the Threats and Vulnerability Working Groups - were "horizontal" in nature, while the other seven were focused on risk assessments in specific sectors. The risk assessment included all the areas where money laundering risk has occurred in Estonia, including, for example, crowdfunding, which, according to the Money Laundering and Terrorist Financing Prevention Act, has not been previously included among the obligated sectors.

FIU invested a lot of resources in the NRA: all NRA working groups had a FIU representative and several working groups were chaired by FIU staff. The FIU was also represented on the NRA steering group. We have provided methodological support to the NRA and FIU data was an important NRA input. The NRA was completed in the spring of 2021 and was published in the website of the Ministry of Finance in May 2021..

1.2. Changes in the legislation

The topicality and tension related to the issues of money laundering, terrorism and non-proliferation financing is reflected by the fact that, in 2020, as many as five different versions of the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) entered into force in Estonia. Various changes were made: the mandatory requirements of Directive 2018/843 of the European Parliament and of the Council

(the so-called V Money Laundering Directive) were adopted; changes related to the establishment of the Financial Intelligence Unit as a separate authority were made; and amendments were made to provisions that had been found to be insufficient or needed clarification.

The main amendments include:

- **The circle of obliged entities was expanded and specified:** art dealers were added to the list of obliged entities (MLTFPA §2 (1) (15); and virtual currency service providers were grouped under a single concept (previously, a distinction was made between virtual currency exchange service providers and wallet service providers) (MLTFPA §10). The conditions under which MLTFPA applies to real estate agents were also specified (MLTFPA §4 and §41).
- The **definition of money laundering** was amended, by deleting the reference to the requirement that the fact of the criminal activity or participation therein, must be established (MLTFPA § 4).
- The **regulation related to beneficial owners** and control thereof by obliged entities was amended (MLTFPA § 9).
- The **regulation related to politically exposed persons** was amended (MLTFPA § 91).
- The principles related to cooperation and the exchange of information between **obliged entities** were amended (MLTFPA § 16).
- The **requirements for the contact person** of the obliged entity FIU were strengthened (MLTFPA § 17).
- The obligation of the **providers of a virtual currency service** to apply **due diligence measures** was made stricter, and the **circumstances related to the object of inspection** were supplemented (MLTFPA § 70-75).
- Situations deemed to **increase risks** were further clarified (MLTFPA § 37 (2)).
- The principle of the **protection of originator of report** was further clarified (MLTFPA § 521).
- Changes were made related to the establishment of the **Financial Intelligence Unit** as a separate entity (MLTFPA § 981).
- Established the principle of a **reporting obligation** for the entities under the supervision of the FIU (MLTFPA § 541).

The provisions of the MLTFPA that have been amended and entered into force contribute to a more efficient and appropriate anti-money laundering and anti-terrorist financing system and harmonise Estonia's anti-money laundering principles with those of the European Union and the FATF.

1.2.1. The reorganisation of the Financial Intelligence Unit into an independent institution

The transfer of the FIU from being a structural unit of the Police and Border Guard Board (PBGB) to being administered by the Ministry of Finance became more widely known in the summer of 2020, when the corresponding amendment was submitted for the draft Act on Amendments to the Money Laundering and Terrorist Financing Prevention Act and Other Acts being processed. It is worth mentioning that an amendment concerning an independent FIU was already being considered in the early 2000s, but at that time it stalled. The intense international focus on the prevention of money laundering and terrorist

financing, including the disclosure of large-scale money laundering cases involving Estonia, caused the amendment to be included in the agenda again in 2019. In terms of preparing for institutional change, 2020 was a very busy year for the FIU team and the Ministry of Finance, which is the responsible for the relevant policy area, as well as for the Police and Border Guard Board (PPA) and the Information Technology and Development Centre of the Ministry of the Interior (SMIT), which manages the IT solutions for FIU.

The establishment of the FIU as a separate authority will help to ensure greater independence and autonomy, which is a fundamental principle of the operation of the international Financial Intelligence Unit. An additional impetus for the change is the opportunity to increase the resources and capabilities of the FIU, primarily the upgrading of IT tools and increasing the staff.

In the heart of the transfer of the FIU was not the amendment of existing laws, because, based on the structure of the FIU, many of the necessary legal principles had already been formulated. Primarily, it was the regulations and other minor legislation that needed to be amended or drafted, along with various guidelines and cooperation and data exchange agreements between agencies.

1.2.2. Changes in the virtual currency services sector

Several important legislative changes concerning virtual currency service providers enabled the FIU to significantly reorganise the virtual currency market. During 2020, the FIU revoked a total of 1,808 authorisations for the provision of various virtual currency services. These included 929 virtual currency exchange authorisations, 868 wallet authorisations (although fewer companies were actually affected, as most that lost their authorisations had both virtual currency exchange and wallet authorisations). In 11 cases, the authorisations were revoked from newly established virtual currency service providers (as of March 2020, this is the general term designating the service).

The reorganisation of the virtual currency service provider market was essential in order to reduce the risks posed by cases of suspected fraud and money laundering related to these providers authorisation in Estonia. Due to the latter, the Estonian business environment has suffered significant damage to its reputation, while the companies committing the fraud were mostly foreign-owned, in many cases from Eastern Europe, and the companies often had only a formal connection with Estonia. Therefore, the 2020 amendment to the law stipulates that the place of business of service providers must be located in Estonia. This has made it possible to remove companies with no real connection to Estonia from the market, and could, therefore, not be properly supervised. However, it has become clear that stricter requirements are insufficient and very little transparency exist in this area. It is important to rapidly reduce the attractiveness of the virtual currency environment for crime, as well as money laundering and terrorist financing. Despite the changes in the law, the risks associated with the virtual currency sector are very high and it is likely that the level of diligence of companies will not increase drastically. Nevertheless, the FIU has noticed positive developments related to compliance with the sector's reporting obligations: in 2020, there were approximately three times fewer companies on the market compared to 2019, but almost three times more companies submitted reports to the FIU (16 reporting companies in 2019 vs. 45 in 2020).

In September 2020, the FIU Strategic Analysis Unit completed **a study of the virtual currency sector**¹, which provided an overview of legislation, services and market participants related to virtual currencies in Estonia. The risks associated with money laundering and the terrorist financing of virtual currencies

¹ <https://www.fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee>



were also analysed, as were the schemes and practices of illegal use of virtual currencies. The FIU concluded that the sector is open to abuse, and therefore, continued vigilance by investigative and legislative bodies is necessary in the area of virtual currency in regard to both in the licensing and supervisory processes and regulation of the sector should be strengthened further. Risks could significantly be mitigated if, among other things, a reporting obligation were introduced, for instance, regarding due diligence measures applied in the sector, the customers of the service providers, and the turnover of brokered transactions. Additional safeguards should also be introduced to protect individuals and their assets, i.e., minimum standards for cybersecurity, information systems and data processing.

1.2.3. Establishment of reporting obligations

In 2020, the Parliament of Estonia, Riigikogu, decided to introduce a new provision into the MLTFPA (§ 541, which entered into force on 1 January 2021), which established the principle that all obliged entities submit reports to the FIU. The content of and submission procedure for the reports shall be decided by the Minister of Finance. The Minister's current regulation requires credit and financial institutions that already submit reports to the Bank of Estonia, to also submit the same reports to the FIU. In order for the **FIU to perform its strategic analysis function** data from obliged entities must be collected analysed and verified via periodic reporting, thereby helping to identify methods, patterns, trends and trends in money laundering and terrorist financing. By effectively conducting strategic analyses and implementing the results, it is possible to intervene in the activities of money launderers and terrorist financiers in a timely manner, and to more effectively prevent the flow of criminal cash flows through the Estonian financial system. Well-functioning strategic analysis also has a preventive function because public information campaigns raise risk awareness among all the parties involved in the anti-money laundering system.

1.3. Feedback for the reporting entities

In April 2020, the FIU sent feedback reports dealing with compliance with the reporting obligation to all market participants for the first time. In addition, the FIU sent more detailed individual feedback to eight major obliged entities. The feedback reports are based on the analysis of the reports submitted by the obliged entities to the FIU during 2019. Sector-specific feedback reports were prepared by the FIU for credit institutions, financial institutions, virtual currency service providers, gambling operators, traders and real estate agents, and other specific non-financial corporations and professions (obliged entities that are consulting sector and public officials). The FIU also provided separate feedback about the latter to the Chamber of Notaries, due to the significant increase in notaries' reporting activity in 2019.

Sector-specific feedback was sent to 17 trade associations and umbrella organisations and via the Register of Economic Activities to all enterprises that have the authorisation, including financial institutions, foreign exchange service providers, virtual currency service providers, gambling operators, corporate service providers and companies involved in the purchase and wholesale of precious metals, gems – a total of 1,793 enterprises operating on the basis of an authorisation.

The FIU feedback initiative was well received by the market participants. By June 2020, the FIU had received reports from all the sectors, including market participants' associations as well as individuals. At the same time as compiling the yearbook, the FIU prepared both sector-specific and individual feedback reports for the 2020 reporting entities, wherein the expectations and recommendations shared by the market participants in the first feedback round were taken into account.

1.4. IT developments in the Financial Intelligence Unit

In 2020, the FIU continued to develop the FIU's information system RABIS, which was introduced a year earlier, in cooperation with the developers of the Information Technology and Development Centre (SMIT) of the Ministry of the Interior. The developments were focused on improving the user-friendliness of the information system, the automation of the data processing and the improvement of the data quality. We increased the information system's ability to automatically receive messages and created new mass processing solutions to reduce the manual work. In order to improve report quality and strengthen cooperation between the obliged entities and the FIU, a flash report function was completed in the spring of 2020, which enables the FIU to provide direct feedback and guidance to the obliged entities. We conducted security tests on the web report form, and based on the results, will continue to improve web report in 2021. We invested in the performance of the information system to ensure its sustainability in the future. The greatest development in 2020 was **interfacing the e-Arrest system with the FIU information system**, the main functionality of which was completed in the autumn. The system has become an important tool for FIU officials and its introduction has significantly accelerated the exchange of information between the FIU and the banks. At the end of the year, money was allocated to the FIU from the European Union Structural Funds for the FIU to make a preliminary analysis regarding the development of additional functionalities in the field of information processing and process automation. This preliminary analysis will be started in 2021.

1.5. Preventing the exploitation of crowdfunding platforms

In 2020, the FIU increasingly received tips suggesting that scammers were using local crowdfunding platforms to defraud money from bona-fide investors. The FIU helped identify a number of possible criminal schemes involving crowdfunding platforms, which led to criminal proceedings.

The crowdfunding platform, **Kuetzal OÜ** collects money from various investors and re-invests it in projects advertised on the website. According to Financer.com², Kuetzal is a new crowdfunding platform that allows anyone to invest in European companies and start-up projects, with an estimated annual return of up to 21%. The creator of the portal is Kuetzal OÜ, a company registered in Estonia. Project owners allegedly receive investments in order to carry out their projects, and thereafter, gradually start repaying them like regular loans. The investors are allegedly repaid a portion of their investment each month, along with the earned interest income. In the case of Kuetzal, the suspicion of fraud is based on the fact that, in addition to actual projects, the clients were also presented with fictitious investment opportunities.

Both Estonian and foreign citizens have invested in various investment projects offered to the public on the **Envestio SI OÜ** website. In 2020, the company's website (online platform) was closed down. People who had invested in the projects sent complaints about the company's behaviour to the FIU. There is also a wealth of information available from public sources indicating that people who have invested money through the Envestio platform have not received their money and understand that they have been cheated.

Information also reached the FIU regarding the activities of a third Estonian crowdfunding platform called **Monethera Group OÜ**, where the money received from the victims of suspected fraud was quickly moved to various countries. In addition, the FIU assisted in identifying the violations committed by the **Savings and Loan Association Erial**³ by mediating information from foreign countries.

² Financer.com is an international economic information and comparison portal, with the goal of providing an overview of various financial services.

³ The Central Criminal Police is investigating investment fraud and embezzlement, and it is also suspected that the management of ERIAL bribed an employee of the Police and Border Guard Board's internal control. (online: <https://www.err.ee/1159975/ko-ko-aaspollu-olgem-hoiu-laenuhistute-suhtes-ettevaatlikud>)

1.6. Analysis of the ex-post reports submitted by the Estonian branch of Danske Bank A/S

In 2020, the FIU continued working on the systematic analysis of the past transactions related to the Estonian branch of Danske Bank. Cooperation has taken place both domestically and internationally and in 2020, the FIU continued to be involved in the criminal proceedings related to the activities of the Estonian branch of Danske Bank.

The FIU has analysed information provided by the Danske Bank in recent years related to customers of the Estonian branch of Danske Bank and hundreds of thousands of transactions with the aim of creating an overview of the information known to the FIU, including the persons and companies, related countries, suspicious transactions and their content. The FIU have created almost 50 files and made almost 60 inquiries in 25 foreign countries in order to check criminal references.

By the end of 2020, the FIU had nearly completed its analysis in the Estonian branch of Danske Bank.

1.7. The Financial Intelligence Unit participation in the Egmont Group project

In 2019, the Egmont Group started an international project called *Conclusions from Large-Scale Cross-Border Money Laundering Schemes*, which was led by the German Financial Intelligence Unit and in which the FIU actively participated. The project aims to bring together the knowledge and practices of the financial intelligence units in various countries, in order to initiate debate and develop possible approaches to identifying networks and patterns of cross-border money laundering, to analyse existing data and develop indicators, typologies, case studies and other tools, in order to facilitate money laundering prevention. The FIU has provided input on potential front companies, contributed to the development and testing of suspicious transaction indicators, and helped create a collection of case studies. The project results were also included in a review called *Trade Based Money Laundering: Trends and Developments*⁴ published by the FATF in December 2020.

⁴ <http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-trends-and-developments.html>



2. A REVIEW OF THE FINANCIAL INTELLIGENCE UNIT'S WORK RESULTS IN 2020

2.1. A review of the reports received by the FIU and their analysis

In 2020, FIU received 8,291 reports (Figure 1), which was an increase of more than 2,100 reports compared to the previous year. The number of suspicion-based reports increased significantly.

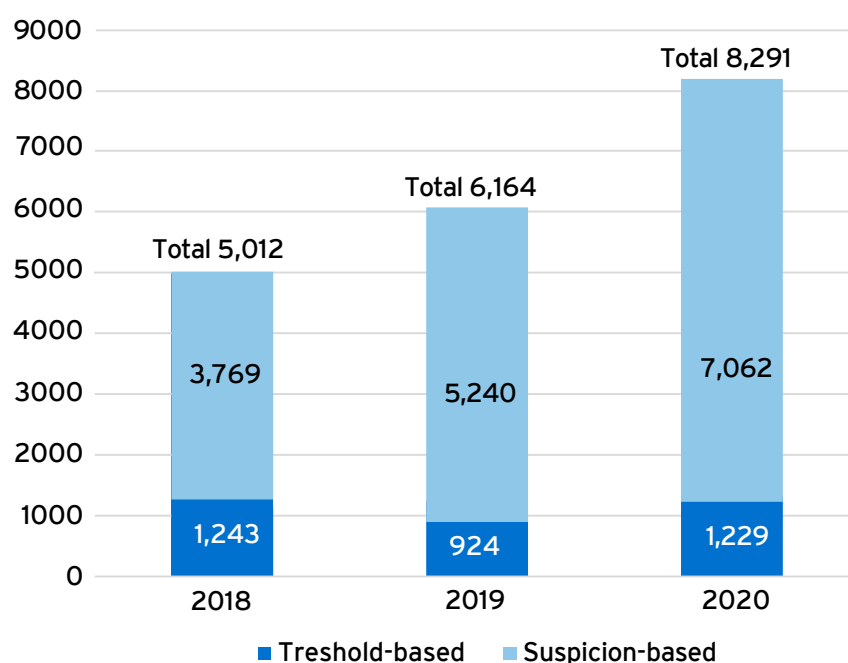


Figure 1. Number of reports received by the Financial Intelligence Unit in 2018-2020

Note: The threshold-based reports also include the ones in which the reason for sending the report is not indicated. The suspicion-based notices also include the queries sent to the FIU.

The number of XBDs sent from EU Member States via cross-border dissemination also continued to increase rapidly: there were 20 such reports in 2017, about 1,700 in 2018, more than 4,000 in 2019, and more than 7,000 in 2020 (Figure 2).

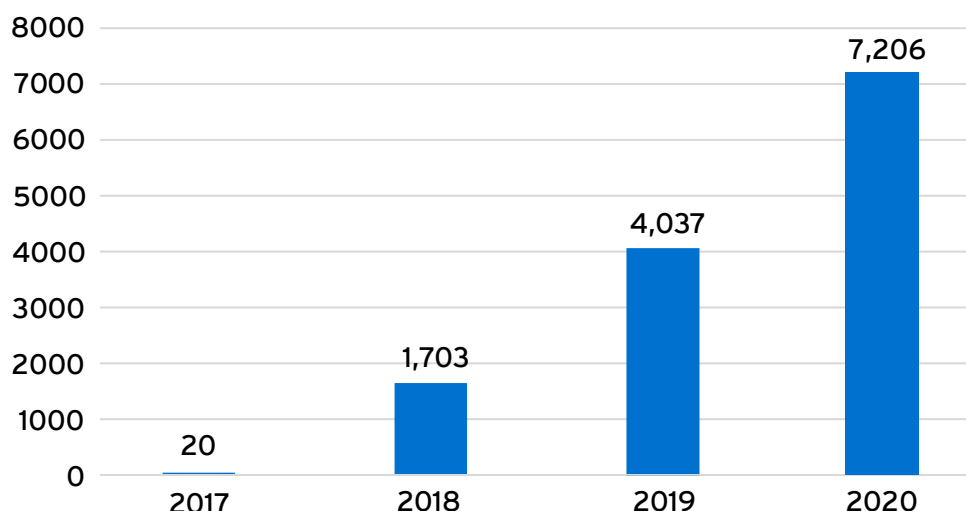


Figure 2. The number of XBDs received by the Financial Intelligence Unit in 2017–2020

Three-quarters of the reports sent to FIU in 2020 were suspicion-based, 15% were cash reports and a tenth were inquiries (Figure 3). This distribution is similar to the previous year, 2019. Suspicion-based reports were dominated by reports related to suspicions related to money laundering, i.e., reports on suspicious transactions (STRs), reports on unusual transactions (UTRs) and reports on unusual activity (UARs). The FIU received ten reports of suspected terrorist financing and 52 reports included suspicions related to the International Sanctions Act.

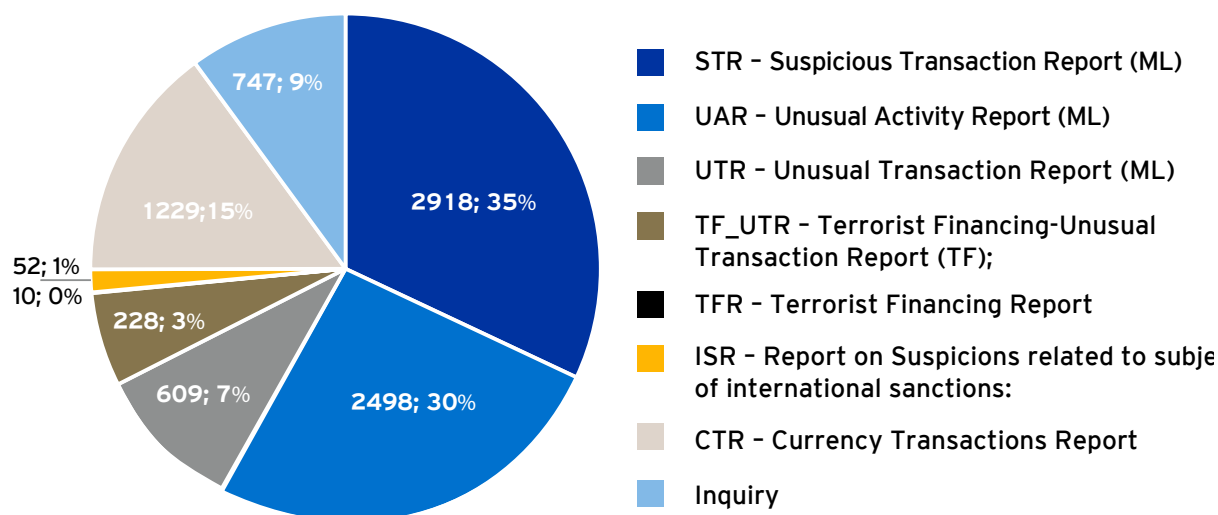


Figure 3. Suspicion-based and threshold-based reports in 2020

In 2020, as in previous years, the FIU received the most reports from credit and financial institutions (Table 1). The share of reports received from credit institutions has increased in the last three years. In absolute terms, the growth has also been noteworthy: in 2020, FIU received 50% more reports from credit institutions than in 2018. The main reason is the increase in the number of reports related to suspected fraud on the one hand and the numerous retrospective reports on money laundering by Danske Bank from the other hand. Compared to the previous year, the number of reports received from financial institutions, virtual currency service providers and non-obliged legal entities increased in 2020, but the

number of reports received from gambling operators and professionals decreased significantly. In the latter case, one of the reasons for the decrease in reporting activity is the link between countries at risk of terrorist financing and the decrease in reports of unusual activity (so-called TF_UTR), because the FIU has instructed reporting entities to report only if in addition to the person's risk country background there is also an additional risk of unusual activity.

Table 1. Distribution of reports sent to FIU by reporting entities in 2018-2020

	2018		2019		2020	
	Reports	% of reporting entities	Reports	% of reporting entities	Reports	% of reporting entities
Credit institutions	2,208	44.1	2,905	47.1	4,594	55.4
Financing institutions	1,360	27.1	1,188	19.3	1,444	17.4
Virtual currency service providers	7	0.1	400	6.5	530	6.4
Gambling operators	279	5.6	250	4.1	118	1.4
Other obliged entities	85	1.7	75	1.2	175	2.1
Agencies and persons from other countries	541	10.8	519	8.4	585	7.1
Public agencies	266	5.3	231	3.7	284	3.4
Professionals	223	4.4	506	8.2	307	3.7
Legally non-obliged entities	43	0.9	90	1.5	254	3.1
TOTAL	5,012	100	6,164	100	8,291	100

In 2020, credit institutions clearly dominated as senders of money laundering-related reports (STRs, UTRs, UARs). Only a few (ten in total) of the reports sent to the FIU were directly related to suspicions of terrorist financing. Most of the reports related to terrorist financing came from financial institutions in connection with transactions with or from countries with a higher risk of terrorist financing (so-called TF_UTR-type reports). The majority of amount-based reports also came from financial institutions. There have been no significant changes in these trends in recent years. However, the number of TF_UTR reports sent by virtual currency service providers did increase in 2020. This is a welcome development, with reports suggesting that some market participants have also improved customer monitoring. On the other hand, market participants in this sector also sent TF_UTR reports to the FIU in 2020, for which the only motive was that the person has the risk country background.

As mentioned above, the number of reports sent by virtual currency service providers increased significantly compared to previous years. The circle of reporting entities also diversified considerably: in 2019, 16 virtual currency service providers sent messages to the FIU, in 2020 already 45 did. If, in previous years, virtual currency service providers have sent only a few reports related to terrorist financing to the FIU, in 2020, there were a total of 47 reports. In 2020, virtual currency service providers sent reports about suspicions related to subjects of international sanctions to the FIU for the first time. Such a positive development is a sign that the FIU's outreach in the sector has borne fruit and the awareness of virtual currency service providers of their role in combating money laundering and terrorist financing has increased.

The significant decrease in the reporting activity of gambling operators is at least partly caused by the lower frequency of so-called TF_UTR-type reports, because the FIU has instructed reporting entities to include references to the singularity of the case, as well as the characteristics of the country at risk, in

such reports. In 2020, gambling operators and notaries also submitted significantly fewer cash notifications to the FIU than in 2019. This is probably due to the COVID-related emergency situation.

Table 2. Distribution of reports sent to the FIU in 2020, based on the reasons for sending the message and the senders

Type of reporting entity	Notices related to money laundering			Notices related to terrorist financing		ISR	CTR	Inquiry	Total
	STR	UAR	UTR	TF_UTR	TFR				
Credit institutions	2,119	2,026	408	3	2	28	8		4,594
Financing institutions	128	258	33	156		1	868		1,444
Virtual currency service providers	304	76	89	44	3	12	2		530
Gambling operators	18	19	3				78		118
Other obliged entities	23	9	22	7		1	113		175
Professionals	67	20	48	18	2	1	151		307
... Lawyers	6	1							7
... Auditors	5	2	1	1			62		71
... Financial and tax advisers	2	1	1						4
... Other legal advisers			1						1
... Notaries	50	8	41	17	2	1	75		194
... Accounting service providers	1	2	4				14		21
... Company or trust management service providers	3	6							9
Public agencies	30	30	3		3	4	6	208	284
Agencies and persons of foreign country	32	14						539	585
Legally non-obliged persons	197	46	3			5	3		254
TOTAL	2,918	2,498	609	228	10	52	1,229	747	8,291

STR – Suspicious Transaction Report; UAR – Unusual Activity Report; UTR – Unusual Transaction Report; TFR – Terrorist Financing Report; ISR – Report on Suspicions related to International Sanctions; CTR – Cash Transactions Report. The reporting entities are categorised based on their main areas of activity.

In 2020, similarly to 2019, the most common reason for sending money laundering reports was unusual transactions occurring on an account (Figure 4). The next most frequently used indicator was based on a suspicion that the subject of the transaction was the object of fraud or was used for money laundering. The number of such reports increased almost tenfold compared to the previous year: in 2019 there were 185 such notifications, in 2020, there were 1,665. This reflects the general increase in computer-based fraud and cybercrime due in part to the growing prevalence of cybercrime tools, the background of anxiety caused by COVID-19, which encourages fraud, and the vulnerability of new financial technologies. The FIU received the most suspicious fraud reports from a credit institution that is a correspondent bank for several large financial technology platforms.

The FIU has the right to suspend a transaction or restrict the disposal of assets if money laundering or terrorist financing is suspected. In 2020, the FIU restricted access to an account 32 times for 30 days and 15 times for 60 days (figure 5). The total amount of the assets, the use of which the FIU restricted, totalled more than €25 million. On nine occasions, property with a total worth of more than 1.36 million euros was retained by a court order in criminal proceedings.

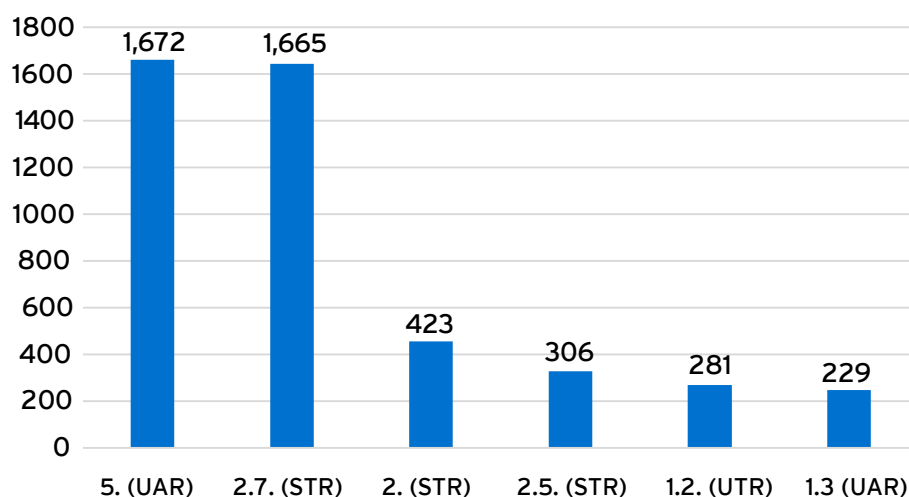


Figure 4. The main reasons for submitting reports on money laundering in 2020.

Explanation:

5. (UAR) Unusual transactions on the account.

2.7 (STR) Suspicion that the subject of the transaction is fraudulent or being used for money laundering.

2 (UAR) Unusual cash transactions not related to a person's normal economic activities.

2.5. (STR) The person does not provide explanations or documents about the transaction to the extent necessary to perform due diligence measures or the submission is not credible.

1.2. (STR) Doubts exist about the veracity of the information provided by the person.

1.3 (STR) A credit or financial institution refuses to enter into a business relationship with a person or terminates a business relationship in accordance with the provisions of §42 of MLTFPA due to the impossibility of performing due diligence measures.

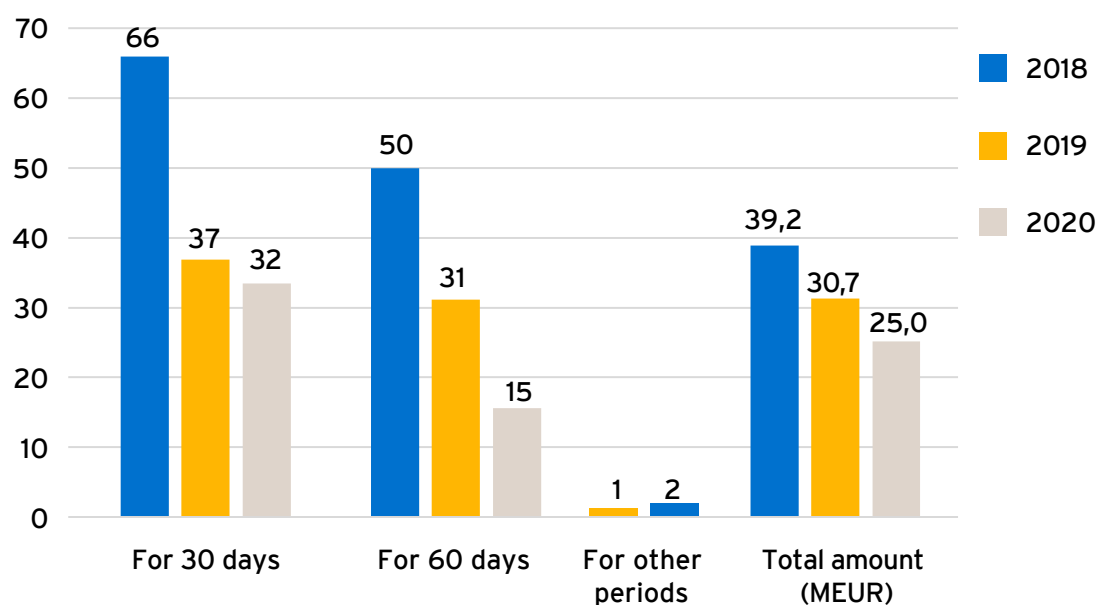


Figure 5. Restrictions on the use of bank accounts imposed by the Financial Intelligence Unit in 2018–2020.

In 2020, the FIU once requested a limit on the disposal of assets for up to one year, and in another case the restriction on the disposal of assets established for six months in 2019 was continued, which was discussed at length in the FIU 2019 Yearbook. In April 2020, the court authorised the transfer of these assets to the state revenue in the amount of €38,726. The FIU imposed an asset restriction of up to one year in the BEC (Business e-mail compromise) case. The fate of the property is still undecided at the time that this yearbook was being compiled, as the FIU restriction expired in January 2021, but the court has yet to decide whether to allow the transfer of the property to state.



In 2020, the FIU restricted the disposal of cash in the amount of €90,900 in one case, a securities transfer transaction in another case, and a real estate transfer transaction in a third case. However, the assets suspected of money laundering were not seized, and these restrictions expired after the deadline.

2.2. National cooperation

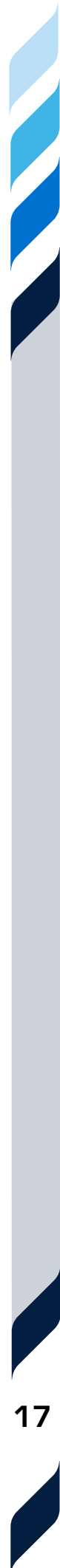
The assignments of the Financial Intelligence Unit include cooperating with obliged entities, competent supervisory agencies and investigative bodies in order to prevent money laundering and terrorist financing. As the FIU's analytical function relies heavily on the information received from obliged entities to prevent money laundering and terrorist financing, it is crucial that the communications between the FIU and the obliged entity is efficient and meaningful.

In 2020, for the first time, the FIU provided both sectoral and large-scale individual feedback to reporting entities (more in chapter 1.3). In addition, we increased operational feedback to reporting entities in order to improve the quality of notifications. In the spring of 2020, the development of the FIU's information system RABIS was implemented, which created the ability to provide direct feedback to the reporting entities based on the preliminary analysis of the reports. Among other things, the operational feedback allows the reporting entity to get a better understanding of what information, and in what form, it needs to provide to the FIU so that the FIU can decide whether or not a suspicion of money laundering exists. This feedback has significantly improved the quality of reporting by the major reporting entities, thereby reducing the need for operational training of the reporting entities in the second half of the year and allowing FIU preliminary analysts to engage more in the in-depth analysis of the reports received.

Based on need, the FIU has held smaller cooperative meetings with obliged entities (credit institutions, Chamber of Notaries), which has improved the quality of the information provided to the FIU, and helped the obliged entities to better understand their role in the anti-money laundering and counter-terrorist financing system.

Another major direction in national cooperation is the exchange of information on money laundering or terrorist financing or related crimes with law enforcement agencies. The cooperation functions reciprocally. Information alluding to criminal activities, which is analysed by the FIU, is forwarded the investigating authority as either a criminal report or information forwarded at its own initiative by the FIU. On the other hand, the FIU also receives information from law enforcement agencies referring to money laundering or terrorist financing, based on which the need for an in-depth analysis of the case is decided. In the case of broader cooperation projects, information exchange and mutual assistance take place in the form of participation in cooperation meetings and through daily communication. As a result of this operational cooperation, the FIU has been able to limit the transfer of seized criminal assets, which have subsequently been seized in criminal proceedings.

An illustrative example of multi-directional cooperation is the case where FIU received information from an obligated person that a customer has fallen victim to fraud, but refused to stop making payments to the fraudsters. The FIU saw that the person had wanted to spend money on investment scams in good faith, and no longer trusted his family members, with whom the situation had been discussed and so they approached the local police in an effort to resolve a situation that would have serious financial consequences for the person. The local police spoke to the individual and the transfers of tens of thousands of euros were suspended. On several occasions, the FIU together with the local police have been able to help the victims of such scams. This shows that those who do not even think about money laundering when doing their daily work, have a role to play in money laundering prevention. In 2020, the number of



cases in which alleged investment offers attracted uninformed people with promises of great returns was regrettably high. By giving criminals the opportunity to use one's current account to move money of unknown origin, one runs the risk becoming involved in a crime oneself.

Financial Intelligence Unit and the Internal Security Service cooperate through mutual professional assistance and the exchange of information in order to investigate transactions suspected of being related to terrorist financing. In addition to information regarding transactions and activities suspected of being related to money laundering, obliged persons also provide the FIU with information on activities suspected of being related to terrorist financing and FIU works closely with the Internal Security Service in these cases. The Internal Security Service verifies the information, and if necessary, the FIU continues to collect additional information from both the obliged entity and foreign Financial Intelligence Units, by making inquiries and imposing restrictions on the disposal of assets suspected of being associate with terrorist financing. This cooperation is essential as the Internal Security Service has its own international network for cooperation and communication on terrorism and the FIU has the capacity to prevent the movement of assets and to obtain the necessary information from the obliged entity without delay.

The FIU's need for national cooperation has not proved itself when dealing with only a few individual institutions or individual cases. The FIU gathers information on suspicious financial transactions, regardless of predicate offences or the location of the money laundering. However, the handling of various crimes is divided between various law enforcement agencies. Therefore, the FIU also have a role to play by calling together various criminal offences when the information indicates that various entities in different location are involved, or different types of crime are being committed by a single group. Criminal cases have been combined based on materials provided by the FIU, in so far as essentially, different episodes of the same criminal case have been committed by the same perpetrators.

The restrictions imposed due to the COVID-19 pandemic significantly impacted FIU's training activities. The number of training sessions and participants was considerably reduced compared to previous years (Table 3). Due to the special situation, several training sessions planned by the FIU for obliged entities were cancelled.

Table 3. Training sessions organised by the Financial Intelligence Unit in 2018–2020.

	2018	2019	2020
Number of training sessions	16	20	4
Number of participants	841	1,223	300

Within Estonia, the FIU cooperates with all investigative agencies. If, based on its analysis, the FIU decides that money laundering or terrorist financing or related offenses may be involved, it forwards the material to the appropriate law enforcement agencies. In 2020, the FIU made a total of 482 such communications to other law enforcement agencies (Table 4). Materials were forwarded on six occasions, in order to decide whether criminal proceedings should be initiated. As of 31 December 2020, the investigating authority had initiated proceedings in four cases, including two cases that seemed that showed signs of money laundering. In two cases, the material sent to the FIU was added to an ongoing criminal case, and in two cases, proceedings were initiated under another section of the law. In reference to these criminal reports, in three cases the alleged predicate offense was fraud, in one case corruption, in one case illegal economic activity, and in one case the offense could not be identified.

Table 4. Materials forwarded to law enforcement agencies by the Financial Intelligence Unit in 2018–2020

	2018	2019	2020
For decisions to be made regarding the initiation of criminal proceedings	52	23	6
– no. of criminal proceedings initiated as of 31.12	36	13	4
– incl. no. of money laundering proceedings initiated	26	10	2
No. to be added to existing criminal cases	95	131	82
Information forwarded at the initiative of the FIU	146	174	210
Answers to inquiries, for information	58	92	184
Materials forwarded for investigation TOTAL	351	420	482
Amounts related to the forwarded materials (€)	1.77 MEUR	3.6 MEUR	6 MEUR

In 2020, 21 criminal proceedings were initiated in Estonia on the grounds of money laundering, two of which were based on material sent to the FIU (Figure 6).

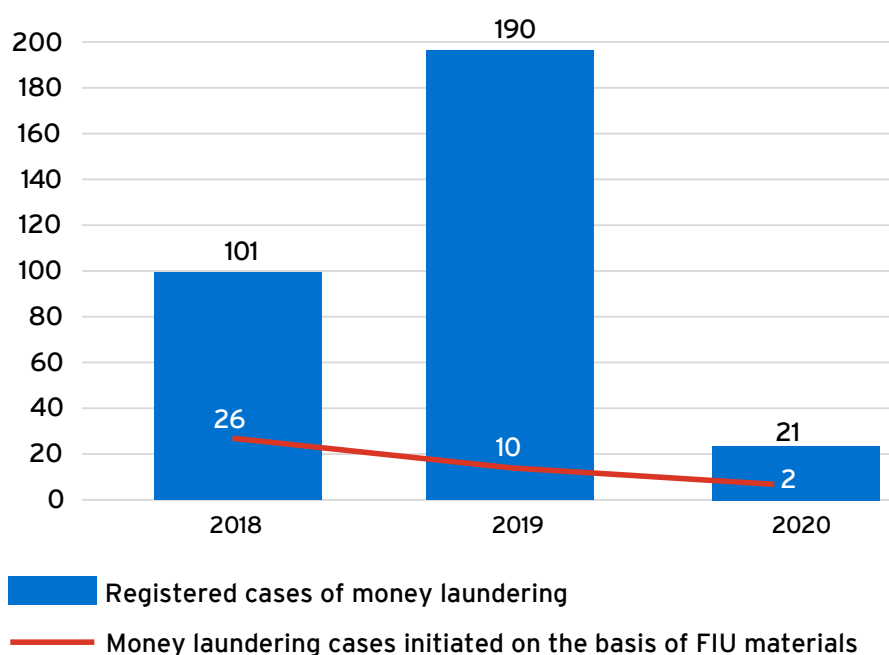


Figure 6. Number of money laundering crimes (episodes) registered in Estonia and number of money laundering and number of money laundering cases initiated on the basis of Financial Intelligence Unit materials sent to investigative agencies in 2018–2020

Note: the information on the number of registered money laundering offenses has been provided by the Ministry of Justice.

The 2019 yearbook stated that the majority of the registered money laundering offenses were committed in the course of two criminal cases, in which the persons partially overlap and which are related to computer fraud cases committed in 2015–2018. In 2020, there were no cases that were similar in scale and the number of registered crimes was significantly lower than in 2018 and 2019. In 2020, the investigative agencies were kept busy with a number of large-scale money laundering criminal proceedings initiated in previous years (including the Danske Bank and GFC Good Finance Company cases), which the FIU was also involved in. Table 4 shows that the number of FIU communications increased significantly, both at the FIU's own initiative and in response to requests made by the investigative agencies.

In 2020, as in previous years, FIU also made the most use of the information in the reports sent by credit and financial institutions (Figure 7).

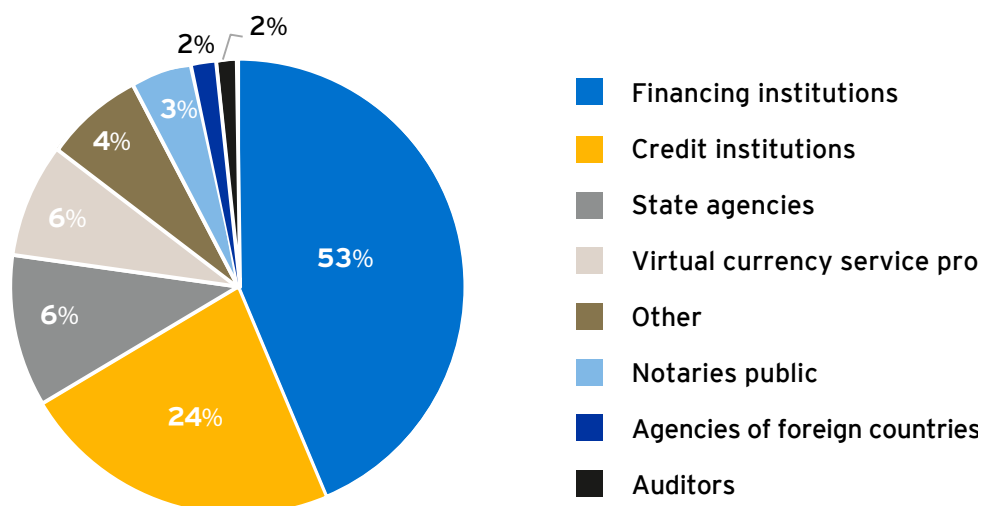


Figure 7. The distribution by reporting group of the notifications used from the materials sent to law enforcement agencies in 2020

One of the most common schemes in 2020 is related to remote or e-identification bank accounts. Opening a remote identification bank account is a convenience for customers. In any case, the total amount of transactions per month for bank accounts opened with e-identification is limited to €15,000. Criminals have also started using e-identification accounts by opening accounts with third-party ID cards unbeknownst to the cardholders. Once they have opened the accounts, they take loans from small and fast loan companies, which are quickly transferred to other accounts, and the money is then withdrawn in cash. The persons in whose names the accounts are opened and the loans are issued become the victims of fraud. A more detailed description of this scheme is given in Chapter 4.

2.3. International cooperation

International cooperation is very important in the work of the FIU. The FIU analyses are mostly based on tracking the money. In order to monitor the flow of money, obtain information on the origin of assets and any possible connections with predicate offences, the assistance of foreign agencies is often required. The FIU can make inquiries to other Financial Intelligence Units, in order to obtain additional information about suspicious transactions and, if necessary, to place restrictions on the disposal of foreign assets. Information from foreign countries can, in turn, help to identify schemes and criminals that are exploiting the Estonian financial system.

We exchange information with our foreign colleagues regarding both topical urgent cases, wherein, in addition to rapid information sharing, partner institutions can also be helped in setting up temporary restrictions on the disposal of assets, and more thorough financial investigations can also be conducted simultaneously with criminal proceedings. Operational cooperation between EU member states is conducted via FIU.net, and we also exchange information with colleagues from third countries through the Egmont Secure Web. Often, the cases being analysed are still in the phase where confirmation is still being sought for suspected money laundering.

The volume of the FIU's foreign cooperation, in particular the number of requests sent by the FIU (Figure 8) has greatly increased. In 2020, the FIU received 460 foreign inquiries from a total of 53 countries,

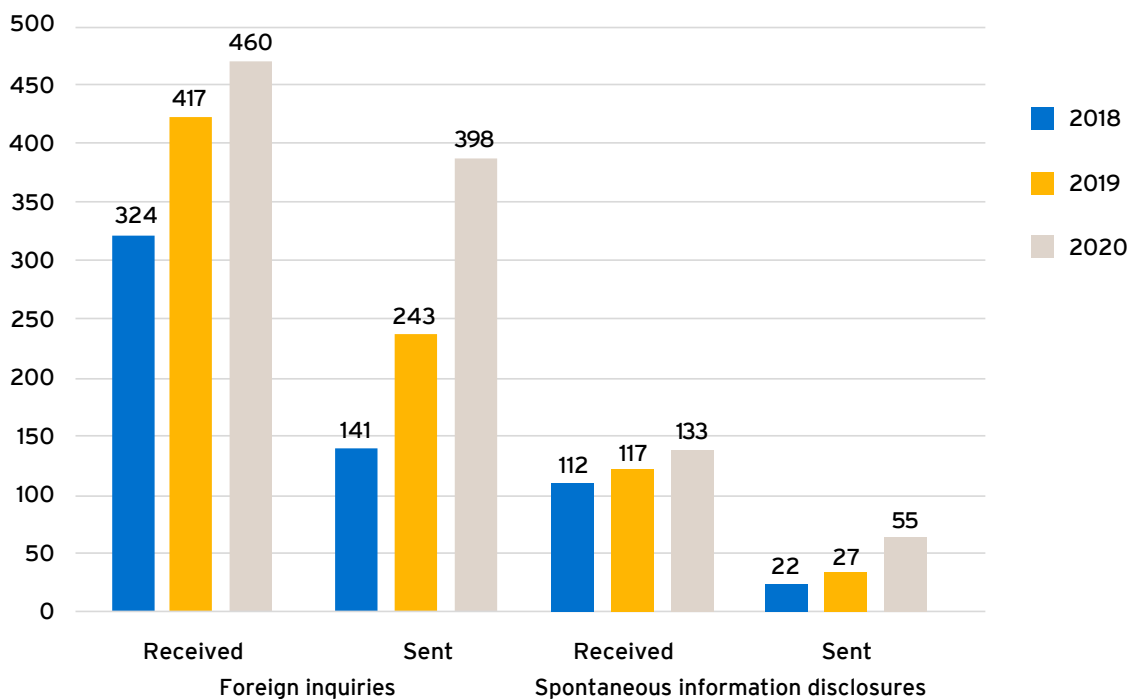


Figure 8. The number of foreign requests received by the Financial Intelligence Unit and sent to the data office, as well as spontaneous information disclosures in 2018–2020

and in turn, sent 398 inquiries to 47 foreign countries. Foreign countries provided information to the FIU on their own initiative (spontaneous information disclosure) 133 times, and the FIU provided information to a foreign country on its own initiative on 55 occasions. The large number of inquiries that were received and the sending of so-called spontaneous information indicates the cross-border nature of money laundering offenses. And also, that the FIU is contributing to the fight against money laundering and terrorist financing, not only domestically but also internationally. In 2020, the average FIU response time for foreign inquiries was 14.5 days, while the responses to the FIU's foreign inquiries were received within an average of 29 days.

In 2020, as before, cooperation continued to be the most active with Estonia's closest neighbours. The most foreign inquiries came from the law enforcement agencies in Finland (72), Latvia (54), Lithuania (39), Germany (30) and Russia (24). The largest number of inquiries were sent from Estonia to colleagues in Lithuania (47), Latvia (35), Germany (30), the UK (25) and Finland (21).

In 2020, the FIU had the closest cooperation with Ukraine, Belarus, Russia, Italy, Finland, Latvia and Lithuania. Inquiries were received, for instance, from Cambodia, Namibia and Kyrgyzstan. Inquiries from former republics of the Soviet Union, which are usually investigating corruption and money laundering related to embezzlement, have increased, whereas most of these events occurred many years ago. The more extensive and important analyses continue to be related mainly to Ukraine, Russia and Belarus.

In 2020, the number of foreign inquiries concerning Estonian companies with FIU authorisation increased significantly (more about the authorisation in Chapter 2.5). In many cases, these companies had already lost their authorisations, or are in the process of having them revoked. As a rule, the connection of these companies with Estonia is minimal although they are registered here. They do not operate in Estonia, do not have current accounts in Estonia and the persons behind the company are either e-residents or foreign citizens who do not reside in Estonia. The emergence in foreign inquiries of these Estonian companies, which are possibly shadow companies set up for criminal purposes, is not only of concern for the companies holding FIU authorisations, but is also a general trend. This illustrates the problem that Estonian companies and Estonian e-residency are being used to commit crimes elsewhere

in the world. Inquiries are mainly sent to the FIU in connection with various types of fraud cases (investment fraud, BEC fraud, computer fraud, etc.). These crimes were also behind the large increase in the number of foreign inquiries in the second half of 2020. A typical case involves money fraudulently obtained in another country which is then transferred to an Estonian bank account opened by a payment service provider or virtual currency service providers registered in another country. Thereafter the criminal proceeds in these accounts were converted into virtual currency on the same day or the following day. Virtual IBAN (VIBAN) accounts, which are so-called technical accounts for the payment service providers, have started to appear as a new concept in the work of FIU. From the viewpoint of a credit institution, a VIBAN account is not a separate account, which means that the bank does not have an overview of the details of VIBAN account transactions and must request such information from its customer who is a payment service provider. Fortunately, the availability of information on VIBAN account transactions has changed rapidly, and effective cooperation has been achieved between Estonian banks and various cross-border payment service providers. In many cases, it is possible to block the fraudulently acquired money that has been transferred to Estonian VIBAN accounts before it is transferred to virtual currency wallets. The money is returned to the victim, if the victim, of course, has filed an application with his or her bank. Another positive development is that banks have carried out on-site inspections of their customers in the presence of the payment intermediaries that are their customers, and one of the banks has terminated its relationship with a customer due to shortcomings in the field of anti-money laundering. The FIU's summary of foreign cooperation in 2020¹ (2020. aasta väliskoostöö kokkuvõte, available in Estonian) was completed in early 2021 and provides a comprehensive overview of the words, schemes and cooperative trends in the external inquiries sent to FIU in 2020.

The FIU also received many inquiries related to fraud from Estonian investigative agencies, mainly from police prefectures, which requested FIU's assistance in obtaining information from foreign countries. In 2020, FIU also made inquiries that assisted the Central Criminal Police, the Internal Security Service and the Tax and Customs Board by collecting the financial information necessary for criminal investigations.

As a positive trend, it is worth mentioning that many of the Estonian bank accounts about which foreign countries have requested information regarding money laundering are already closed in Estonia, and the banks have also notified the FIU. At this point, we'd like to praise the banks for their efficient work!

The dissemination of XBDs between EU Member States has intensified, although both national dissemination practices and the content of such notifications are inconsistent. Some of XBDs received by the FIU have provided valuable information, and have prompted further case studies. Estonia is also receiving more and more inquiries that have been prompted by our XBDs, as well as from our spontaneous information disclosures, the main inputs of which are the notifications submitted by our obliged entities.

In general, the more automated and harmonised the system for exchanging messages and spontaneous information is between the countries of the European Union, the more it benefits the anti-money laundering system. Hopefully, a new body, i.e., the European Financial Intelligence Unit, will soon be coordinating EU-wide issues. At the end of 2020, a steering group of EU member states submitted a draft document for the establishment of an EU-wide money laundering institution to the European Commission, which in turn will make a proposal to the Council of Europe to establish a so-called Co-ordination and Support Mechanism (CSM) in the second quarter of 2021. The draft does not prescribe what the new agency should be, but rather describes its needs and opportunities. As the name of the new agency indicates, it will be a support and coordination unit, rather than the EU's central Financial Intelligence Unit, which would gather operational data from all countries.

¹ <https://fiu.ee/media/121/download>

2.4. Supervision

The FIU's statutory task is to supervise certain market participants at national level. The monitoring tasks assigned to the FIU are prescribed in the Money Laundering and Terrorist Financing Prevention Act and in the International Sanctions Act. In 2020, the FIU Supervisory Authority conducted 44 off-site inspections and 30 on-site inspections, including three supervisory inspections under the International Sanctions Act (Figure 9). Misdemeanour proceedings were initiated in 17 cases, the most common violation being deficiencies in compliance with the duty of care.

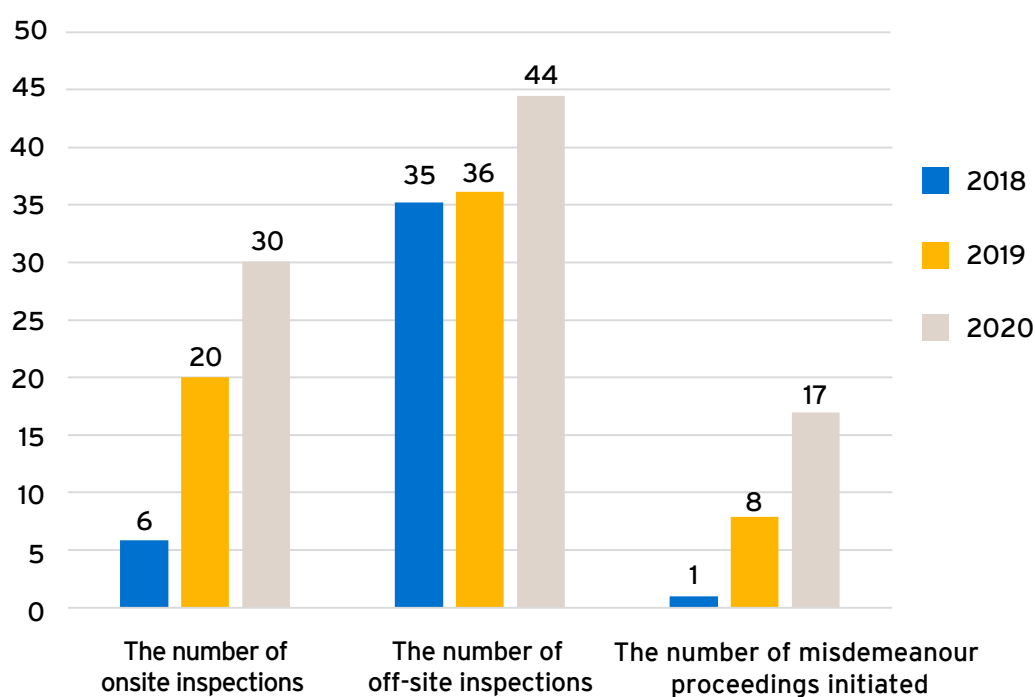
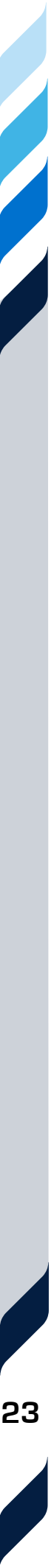


Figure 9. Financial Intelligence Unit's supervisory inspections and misdemeanour proceedings in 2018–2020

In 2020, the FIU focused its monitoring on a broader area of activities, i.e., on the control of real estate brokerage firms, virtual currency service providers, financial institutions, auditors and bailiffs.

Table 5. The distribution of supervisory inspections performed by the Financial Intelligence Unit in 2020, based on the activities of the inspected entities

Fields of activity	Number of inspections
Auditors	15
Financial institutions	15
Virtual currency service providers	13
Real estate agents	10
Bailiffs	10
Buyers and wholesalers of precious metals and stones	4
Traders	3
Providers of trust and company services	2
Credit institutions	1
Payment institutions	1
TOTAL	74



In 2020, the inspection of real estate brokerage companies, which started in 2019, was continued. As the inspections carried out in 2019 revealed that there were several shortcomings in the activities of the market participants, both in the application of due diligence measures and the fulfilment of the obligation to register data, the FIU carried out an additional 10 on-site inspections in the real estate sector in 2020. The shortcomings identified during the 2020 monitoring confirmed that the market participants in this sector need to be monitored in 2021. The results of the inspections indicate that awareness regarding the application of due diligence measures by the market participants in this sector needs to be increased.

In the virtual currency sector, monitoring proceedings were initiated in most cases in 2020, because the FIU had received negative information, i.e., suspected fraud against the customers of virtual currency service providers. The FIU identified deficiencies in the application of due diligence, data registration and storage, and reporting obligations in most of the audited companies. The amendment to MLTFPA, based on which virtual currency service providers have an obligation to locate the company's management board in Estonia, has made it possible to carry out significantly more on-site inspections compared to 2018 among the market participants in this sector. In 2020, the FIU carried out a total of 13 inspections in the virtual currency sector.

In 2020, the FIU also focused to a greater extent on the inspection of obliged entities that have the authorisation of financial institutions, by conducting 15 inspections. As a result of the inspections, it was revealed that many of the companies that had been issued authorisations to operate as financial institutions had not provided any service in Estonia for six months after the authorisations were issued, which enabled the FIU to revoke the authorisations of 13 companies.

In 2020, monitoring also focused on auditors and bailiffs, compliance with the notification obligation to the FIU was checked. As a result of the 15 inspections carried out among the auditors, two companies were found to be in breach of their reporting obligations to FIU, and two companies were issued orders to rectify the deficiencies. The FIU initiated misdemeanour proceedings for breaches of the notification obligation. Ten inspections were carried out among bailiffs, which resulted in one order was issued to eliminate the deficiencies. The results of the monitoring of both sectors indicate the market participants' awareness of their obligation to notify the FIU need to be increased.

2.5. Granting of authorisations

In 2020, the granting of authorisations was a very labour-intensive field of activity. Although the number of applications for new authorisations decreased from 1,690 in 2019 to 749 in 2020, a total of 815 authorisation revisions were processed and 1,844 authorisations were revoked. Of the latter, 1808 were authorisations for the provision of virtual currency services (including a virtual currency wallet service and a virtual currency exchange service).

On March 10, 2020, the revision of the Money Laundering and Terrorism Prevention Act entered into force, which established stricter requirements for the providers of virtual currency services when applying for granting authorisations. These amendments obligated the companies to comply with the new requirements no later than 1 July 2020. If the company had not brought its activities into compliance with the law by the deadline and had not submit the necessary documents, the FIU revoked the company's authorisation(s). Some companies that did not comply with the amendment to the law submitted a notice

of temporary cessation of activities (a total of 373 as of 31.12.2020). A large percentage the authorisations of virtual currency service providers (915 in total) was revoked in the first half of 2020 as a result of the survey of virtual currency service providers, since the investigation revealed that the undertakings had not commenced operations within six months of the issue of the permit or did not comply with the repeated precepts of the FIU.

In 2020, 749 applications for granting authorisations were submitted to the FIU, of which 524 were approved and 195 authorisations were denied (Figure 10).

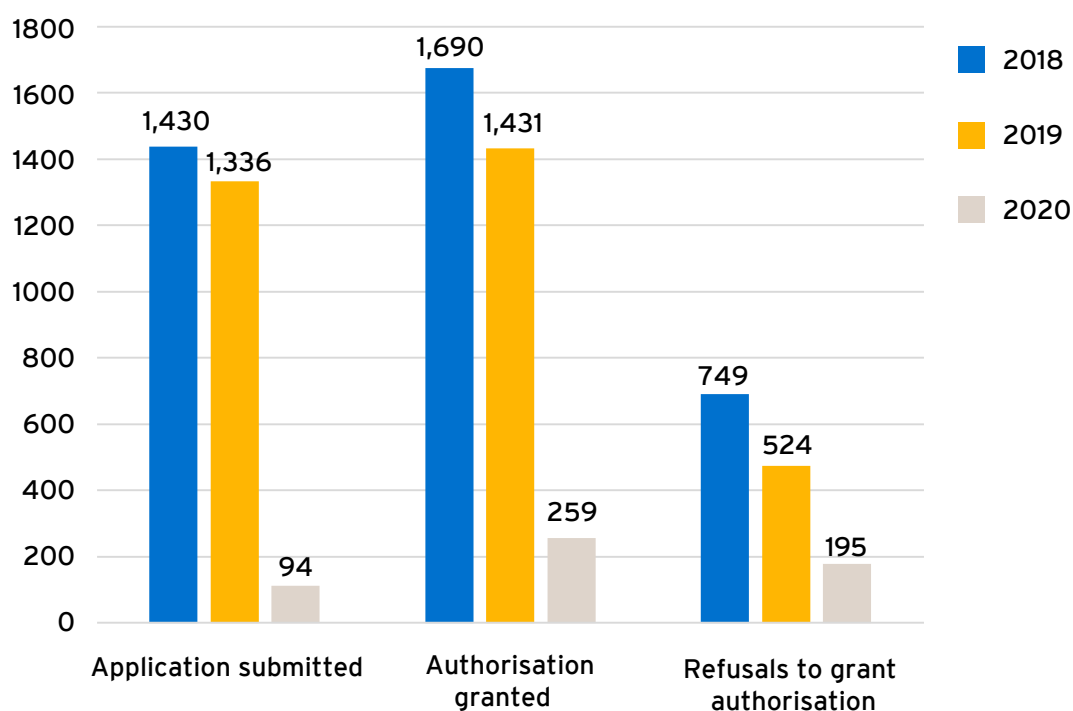


Figure 10. Overview of the applications for authorisations in 2018–2020

Note: As of 1 January 2021, 30 authorisation applications submitted in 2020 were still pending.

The FIU continued to receive the largest number of authorisation applications from virtual currency service providers (Table 6).

Table 6. Distribution of applications for authorisation submitted to the FIU in 2020, based on the business activities of the applicants

Field of activity	Applications filed	Authorisations granted
Financial institution	51	39
Pawnshop	3	2
Trust and company services	46	38
A service of exchanging a virtual currency against a fiat currency	179	163
Virtual currency wallet service	177	162
Virtual currency service	289	116
Buyers and wholesalers of precious metals and stones	4	4
TOTAL	749	524



3. COURT DECISIONS RELATED TO MONEY LAUNDERING IN 2020

3.1. Criminal proceedings

In 2020, ten money laundering judgments entered into force in Estonia: one Supreme Court decision; one circuit court decision; and eight county court decisions. Sixteen people were convicted of money laundering (15 physical persons and one legal entity). In three cases, the predicate offense of money laundering was computer fraud, in three cases business fraud (BEC or business e-mail compromise) and in two cases tax fraud. In 2020, the assets of seven people who were convicted of money laundering were confiscated. A total of about €139,000 was confiscated, in addition to one vehicle and one computer. Eight people were acquitted of money laundering based on decisions by the Supreme Court and a circuit court.

1-15-6497

The circuit court found that **in a situation where a person is accused of money laundering, the object of which is the property obtained by his or her own predicate offence (so-called self-laundering), the concept of money laundering needs to be further narrowed in terms of interpretation.**

For the following reasons:

1) By treating essentially any steps of the perpetrator to conceal the origin of the proceeds of that offense as money laundering, a person would be compelled, under the threat of criminal punishment, to act in a manner which would facilitate the detection of his or her offense. The infringement of the protection against self-incrimination guaranteed by §22 (3) of the Constitution arising from such a threat of punishment would not be, in at least some cases, proportionate and would, therefore, be unconstitutional.

2) The wrongdoing that the perpetrator of a predicate offense commits by concealing the origin of the property obtained from the predicate offense and avoiding its return or compensation, is already included, at least to a certain extent, in the wrongful activity of the predicate offense itself. In cases where the wrongdoing of money laundering is fully exhausted by the perpetrator's earlier predicate offense, punishment for money laundering may lead to a violation of the prohibition on double jeopardy (*ne bis in idem*) prescribed in § 23 (3) of the Constitution.

3) The sanction rulings specified by §394 of the Penal Code must also be taken into account when defining money laundering as being punishable as a criminal offense. Namely, money laundering can be punished by a pecuniary punishment or up to 5 years of imprisonment (§394 (1) of the Penal Code); however, if the money laundering is committed in a group, for at least the second time, or large-scale in nature, punishment can even be imprisonment for two to ten years (§394 (2) of the Penal Code). Given the fact that the circle of predicate offenses of money laundering is not limited, but includes all criminal offenses, such a severe sanction indicates that money laundering itself must have a significant potential to jeopardize the public financial and economic system, which constitutes a qualitatively independent and serious infringement, in addition to the predicate offense. Otherwise, it would not be possible to explain why committing money laundering may, based on the proceeds of crime, be punishable more severely than the predicate offenses by which the assets that were the object of money laundering were obtained. This clearly indicates that the concept of money laundering must be interpreted restrictively, especially in a situation where the concealment of the proceeds of crime is carried out by the perpetrator of the crime who is responsible for the predicate offence.

According to the circuit court, concealment or alteration of property obtained by a criminal offense – especially if committed by the perpetrator of the alleged predicate offense – **shall be regarded as money laundering only if such conduct constitutes a specific criminal intensity and danger to the legal interest protected by legal rights.**

According to the indictment and decision of the county court, the conduct alleged against the accused as money laundering was summarised as follows: Individual A was guilty of the acts described in the allegations of fraud, causing insolvency and committing tax evasion, whereby he received payment (7,509,286 EEK) in his personal bank account and distributed a part of the money (5,075,000 EEK) by making ten bank transfers to company X. Individual A himself was the founder, shareholder and board member of company X. In addition, Individual A made ten transfers totalling 170,000 EEK from company X's bank account to company Y. The founder, shareholder and actual director of company Y was Individual A's life partner, Individual B. Individual A transferred the money from company X's account to company Y's bank account as agreed with Individual B. In addition, Individual B, who was also company X's bookkeeper, in cooperation with Individual A, deliberately left 3,999,137 EEK out of the balance sheet in company X's annual report. According to the charges, such conduct, which is known as the transfer and possession of criminal assets, was intended to conceal and keep secret the nature of the assets and their illegal origin, and to help Individual A, who had participated in the criminal activity, to avoid the legal consequences of his actions.

The circuit court acquitted all the persons accused of money laundering, maintaining that the bank transfers of Individual A described in the indictment and identified by the county court did not impair the orderly functioning of the state's financial and economic system to such an extent that the resulting wrongdoing was not already covered by his alleged predicate offenses. According to the circuit court,

the conduct described in the money laundering accusation of Individual A can be legally assessed as a non-punishable follow-up to his or her alleged predicate offenses, the wrongdoing caused by which is included in the predicate offenses. The Chamber based its view on the fact that neither the indictment nor the county court's decision indicated that the conduct described in Individual A's money laundering indictment was part of any wider, more permanent and universal scheme of conversion and/or concealment of property. According to the court, his alleged money laundering act did not have the complexity and scale that would have given it an independent quality. The conduct described in the money laundering charge only perpetuated the damage that had already been suffered by the victim(s) as a result of the conduct of Individual A, who is considered to be a predicate offender. No independent damage or threat to the orderly functioning of the state's financial and economic system, and more specifically to the insurance of legal economic and monetary turnover, arose from the circumstances caused by the bank transfers of Individual A. Despite the transfers, a traceable connection remained between the person of Individual A and the money received by him. Thus, the assets obtained by the crime, when making the bank transfers described in the accusation, and the recording of false information in the annual report of company X, as a concealment activity, did not qualify as money laundering.

3.2. Administrative court proceedings

All three cases that started in 2019 and continued in 2020, which we highlighted in the 2019 Yearbook, were ended in 2020. One of the most important decisions for FIU in 2020 was Administrative Case No. 3-20-664, in which the Supreme Court made a decision⁵ on 15 October 2020. The restriction of up to one year reported on in the previous yearbook was appealed to the Supreme Court, which made a substantive decision in the matter. It held that the imposition of a restriction on the disposal of up to one year as well as the transfer of property to state ownership is permitted under the conditions specified by law.

Money Laundering and Terrorist Financing Prevention Act, which entered into force in 2017, clarified the FIU's right to set a limit of up to one year and thereafter transfer assets to state ownership. The main change was the amendment to the law that specified the precondition for imposing a restriction of up to one year and transferring property to state ownership is that the account holder is the holder of the assets, and the proprietorship of the account must be proven by the account holder. The need for this amendment to the law arose from the decisions of the Supreme Court made since 2011, in which the opinion of the court was that the assets in the account belong to the account holder, because the person has a claim against the bank. This principle also applied in situations where the account holders themselves confirmed that they were not the owners of the assets.

The problem, which is resolved by the provisions of the new law, arises mainly in cases where, for example, an account is used for fraud and it is impossible to identify the persons who committed the crime in criminal proceedings. In this case, it is important that any assets previously seized in criminal proceedings, which were terminated due to the impossibility of identifying the persons, not be returned to potential criminals or persons related to them. This involves very isolated cases, in which the state can use administrative proceedings in order confiscate assets that cannot be confiscated by criminal proceedings. These are situations which it is known that the origin of assets is illegal and the holder of assets is unable to prove their legality.

⁵ <https://www.riigikohus.ee/et/lahendid?asjaNr=3-20-664/10>



Since 2017, the Financial Intelligence Unit has set three restrictions on use of up to one year, and in two cases, has applied for the right to transfer the property to state ownership. After the transfer of assets to state ownership, the owners of the assets retain the right of recovery for up to three years, if they can prove ownership based on legal grounds.

In 2020, 41 administrative cases were initiated in which the FIU was involved, of which 18 cases were closed in the same year and 23 cases are still pending in 2021. Thus, the number of FIU administrative cases increased from six in 2019 to 41 in 2020. The increase in the number of administrative cases was caused mainly by amendments to the law related to granting authorisations. This mainly impacted virtual currency service providers, in regard to whom the mandatory requirements for issuing an operating license were tightened on 10 March 2020. In addition, the administrative cases impacted the virtual currency service providers that were licensed before March 10th, but had not brought themselves into compliance with the new requirements, not filed the necessary supporting documents by July 1st. The need for the change was based on the fact that many of the Estonian companies that had received an authorisation in Estonia did not operate in Estonia, did not provide services to the Estonian market, and were managed and represented from abroad.

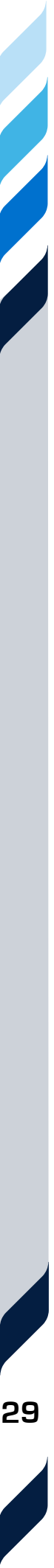
The figures for administrative proceedings are the following:

- Three proceedings resulting in a restriction on the transfer of assets being invoked for up to one year, and permission being granted for the assets to be transferred to the state;
- Two proceedings in connection with financial sanctions;
- Three proceedings in connection with the restrictions on transfers set by the FIU (30 or 60 days);
- One proceeding related to the subject of disclosing information and requesting information;
- 32 proceedings in connection with the revocation or refusal of authorisations, which were divided as follows:
 - refusal or revocation of granting authorisations due to stricter licencing requirements (20 proceedings);
 - other authorisation issues (12 proceedings).

More than half of the concluded proceedings have resulted from the dismissal of the complaint or a compromise being reached between the parties. Of the complaints filed against the FIU, the court upheld only two of the appeals during the substantive proceedings.

Most of the procedures related to granting authorisations were related to the revocation of granting authorisations or refusal to issue activity authorisations because the company's management board was not located in Estonia. This means that companies were mainly managed and represented from abroad, and only the responsible members of the management board as defined by § 17 of MLTFPA were located in Estonia. As most of the complaints were lodged in the second half of the year, few court decisions have entered into force. For example, the completed proceedings related to granting authorisations include the decisions 3-20-1448 and 3-20-1618 of the Tallinn Administrative Court.

The dispute in Administrative Case No 3-20-1448 was based on the applicant's failure to provide, by 1 July at the latest, the necessary documents in order to enable the FIU to assess its compliance with the new requirements. The court agreed with the FIU that the law set a deadline by which all virtual currency service providers had to comply with the new requirements, and in order to prove compliance with these requirements, an application for amendment of one's operating authorisation had to be submitted to the Register of Economic Activities.



The dispute in Administrative Case 3-20-1618 was based on the company lacking a place of business or payment account that complied with the requirements provided by law, which means that the applicant did not meet the new requirements. Thus, the person's application for amendment of the authorisation had to be rejected and the authorisation had to be revoked.

In the previous yearbook, we discussed the dispute with the media group Rossiya Segondya, which is related to international financial sanctions and continued in 2020. In January 2020, Rossiya Segondya filed a complaint with the Tallinn Administrative Court and applied to have the Sugandha freezing of Rossiya Segodnya's payments by the FIU declared illegal, and to have the consequences remedied. The FIU submitted confirmation of the legality of the application of sanctions based on Regulation No 269/2014 of the European Parliament and Council, which deals with restrictive measures related to activities that undermine or threaten the territorial integrity, sovereignty and independence of Ukraine. One of the sanctioned persons under this regulation is Dmitry Konstantinovich Kiselyov, General Director of Rossiya Segondja. Based on the regulation, the assets of persons who are subject to these financial sanctions must also be frozen, and they must be prevented from gaining access to these financial resources. In order to resolve the dispute, the Tallinn Administrative Court wished to apply to the Court of Justice of the European Union for a preliminary ruling. However, this proved to be unnecessary, since on 23 December 2020, the Tallinn Administrative Court issued a ruling terminating the proceedings because the applicant withdrew his complaint.



4. MONEY LAUNDERING SCHEMES

Below is an overview of the most significant or widespread schemes analysed by the FIU in 2020.

Strategic goods

In 2020, the FIU investigated a case based on a suspicion that companies registered in Estonia could be selling strategic goods and providing related services in the amount of €2.7 million. The goods included electronic equipment, software, helicopter parts, mobile shelters, and a hardware programming service. In all cases, the buyers of the goods and services were foreign companies that might be involved in the military sector. It proved to be difficult for the FIU to accurately classify these goods and to assess the need for a license for strategic goods. Therefore, the FIU consulted with other competent national agencies.

For the purposes of the Strategic Goods act, strategic goods include military goods, defence-related products, goods used to commit human rights violations and dual-use items. The control of strategic goods and related transactions is necessary in order to ensure the transparency and legality of the transactions moving through the Estonian economic sector and to prevent the laundering of illegally obtained funds, and the movement of strategic goods through Estonia to sanctioned countries or terrorist organisations. If strategic goods are traded or a related service is provided, it may be necessary to have a special permit issued by the Strategic Goods Commission of the Ministry of Foreign Affairs in Estonia⁶, whose members are representatives of various Estonian state agencies.

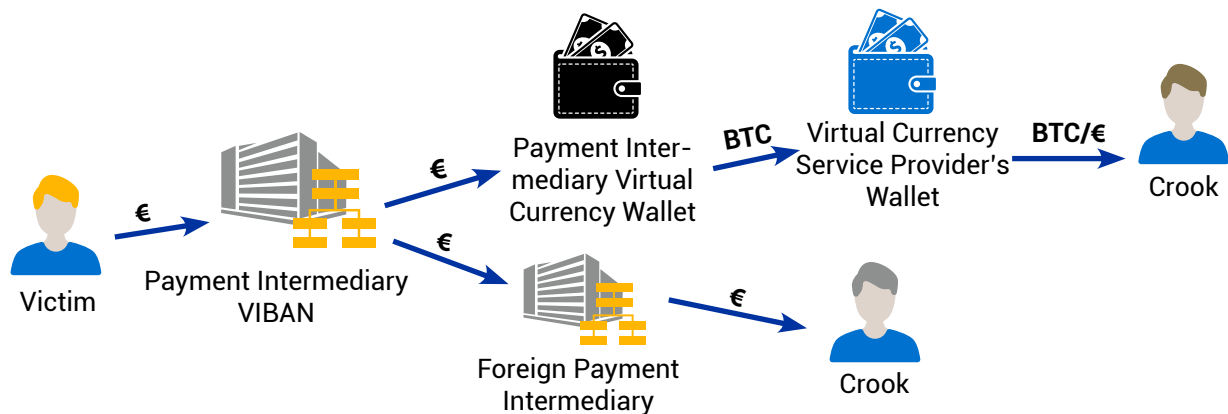
The use of VIBAN accounts

In 2020, the relatively new banking service called Virtual IBAN (hereinafter, VIBAN), attracted the attention of the FIU. In the case of VIBANs, a credit institution issues personalised IBAN account numbers to its customers, which the customers can then distribute to their own customers who become the end users. FIU is aware that VIBAN accounts are generally issued to foreign financial intermediaries that are

⁶ <https://vm.ee/et/strateegiliste-kaupade-kontroll>

clients of a credit institution. The VIBAN account is seemingly similar to a regular IBAN account issued in Estonia (begins with EE, which refers to an Estonian credit institution), and therefore, it is difficult to immediately discern whether the account belongs to a credit institution's customer or a customer of the latter. However, as the holder of the VIBAN account is not a customer of an Estonian credit institution, but a customer of a payment intermediary registered in a foreign country, it is the foreign payment intermediary that applies the due diligence measures to these persons. Thus, it is extremely important that the risk tolerance of the foreign payment intermediary and the correspondent bank of an Estonian credit institution coincide for the most part, so that any attempts to use VIBAN accounts to commit various crimes through the Estonian financial system can be quickly identified.

The FIU has received information (notifications and foreign inquiries) about the use of VIBAN accounts for criminal purposes on more than 300 occasions. The modus operandi is usually, that a legitimate customer makes a deposit in a VIBAN account believing that the account belongs to a private individual and has been opened in a credit institution, and falls victim to a fraudulent transfer of fund by trying to make an investment or as the victim of some other scheme. However, the money that is deposited is quickly transferred from the VIBAN account to a virtual currency wallet or another foreign payment institution. The funds move between various financial institutions within a few hours, usually faster, and by the time the customer realises that this is a scam, the funds have been lost.



Scheme 1. Example of the use of the VIBAN account in criminal schemes

Note: BTC - bitcoin

In conclusion, it should be recognised that very large amount of funds, which were acquired as a result of international crime (mainly fraud), were transferred to other countries in 2020. Therefore, foreign Financial Intelligence Units have made more and more inquiries to Estonia, in order to obtain information as well as limit the amount of money transferred to VIBAN accounts. By the time the inquiries are made, there is little hope of recovering the assets.

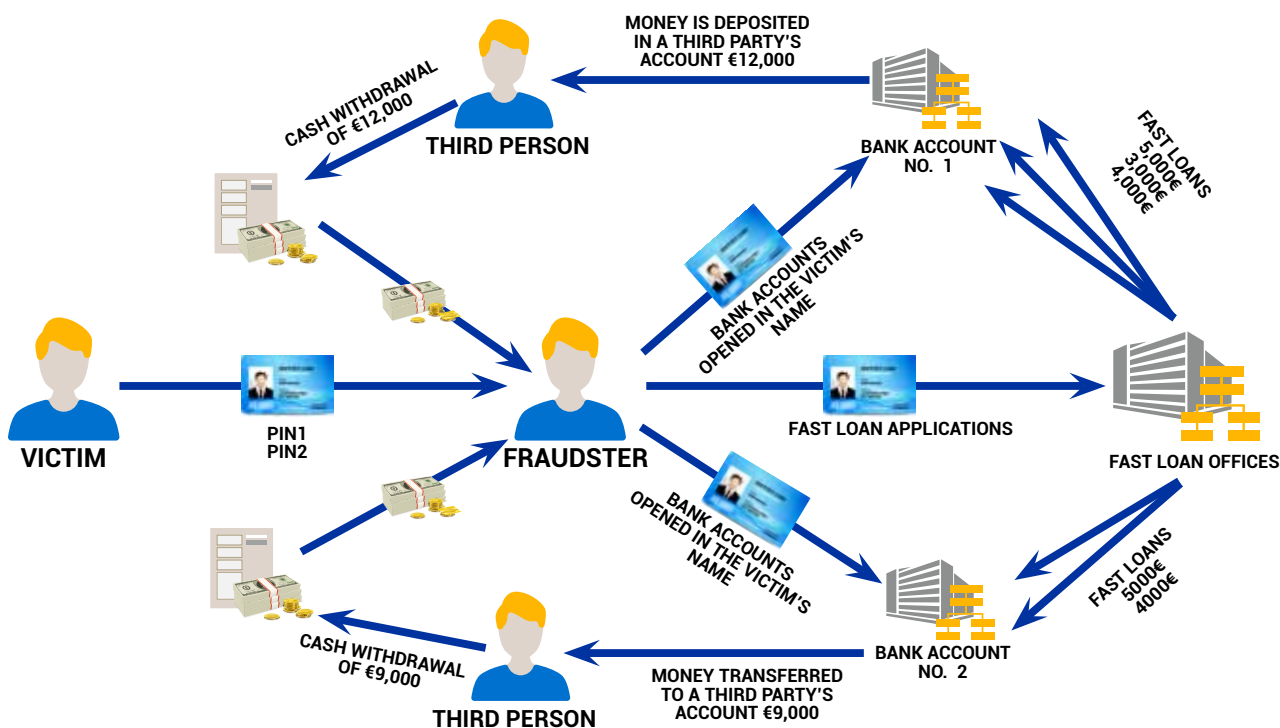
According to FIU, for the reasons described above, the VIBAN service is vulnerable to investment fraud and other cybercriminals and has a high risk of money laundering. When an investment service or other financial service provider controls a VIBAN account from public sources, it learns that the account is with a credit institution that may seem more reliable to a person than a payment institution because it demonstrates less appetite for risk and greater anti-money laundering capacity. Therefore, by feeling certain about the legality of their transaction, or the possibility of recalling one's transaction, if necessary, the potential victim is in a weaker than expected position. In reality, the recipient of the money is a client of the financial intermediary, which can only be identified if the correspondent bank cooperates specifically with its financial intermediary client. However, the person will not find this out until he or she wishes to rescind the transaction.

Frauds

In 2020, the number of reports related to various fraud cases increased (in total, the FIU received more than 1,600 reports mentioning possible fraud). Based thereon, the greatest trend is an identity theft. As a result of identity theft, the victim loses his or her assets, or financial obligations are entered into on his or her behalf. In many cases, the fraud is not revealed until the person receives a collection claim.

The following is an example of a common identity theft scheme. Someone gives their ID card with passwords to fraudsters in hopes of earning easy money or helping a friend. In return, the person is promised €500, so the fraudster can open a business on behalf of the victim, which will later be allegedly sold to a third, non-resident person. Of course, the company is never established. Instead, the fraudster opens bank accounts in Estonian credit institutions on behalf of the victim using e-identification and then uses it to take as many fast loans as possible. The money received is immediately transferred, either directly or through a chain of transactions, to third parties who withdraw the amounts received in cash. In 2020, the FIU imposed a number of restrictions totaling almost €600,000 on similar schemes, in order to prevent the movement of criminal proceeds and to ensure the preservation of funds in criminal proceedings.

In addition, there have been cases where the victim is driven into a state wherein, through skilful persuasion and the promise of a refund, the victim him- or herself commits a crime in hopes of recovering the lost assets. One of the most striking examples is a case whereby someone fell victim to a scam on a foreign investment platform, and thereby lost a large amount of his personal property. With the help of frequent, sometimes daily, phone calls, the criminals persuaded him to transfer more money into the platform in order to recoup the lost assets through a very good investment. As his own assets had been exhausted, he misappropriated a large sum of money from his company's account in an attempt to recover his personal money through a successful investment. The FIU's restriction prevented further damage being caused to the company.



Scheme 2. Example of the fraud by identity theft

COVID-19 related cases

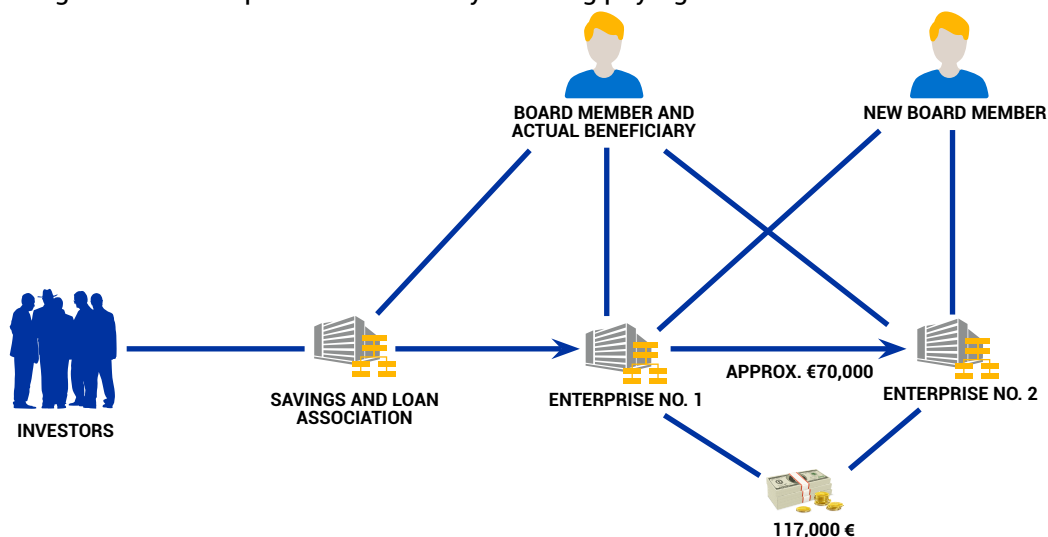
The year 2020 will probably be remembered by many for the spread of the COVID-19 virus, which has also resulted in new trends in crime. Taking advantage of the global pandemic, criminals have found various ways to take advantage of the situation. In 2020, the FIU was confronted with a number of different cases where COVID-19 was the keyword to a greater or lesser extent. For example, there were cases where forged documents were presented to the customer which created a false impression of the quality of the PPE being supplied and PPE was also sold at prices that were significantly higher than the market prices. There were also cases in where it was suspected that promises had been made to supply PPE, but actually there were no plans to do so. The pandemic has also been used as a pretext when committing business scams, for instance, using it as an excuse for why one's business bank account number has changed. Consequently, given the complex global pandemic situation, it is important for companies to be very careful when choosing business partners and to check whether any information provided is true when changing counterparty bank details through various channels (in addition to e-mail, for example by telephone), and if any changes occur in the banking details of the partner, to use various channels (in addition to e-mail, for example, by phone, as well as by e-mail) to ascertain whether the provided information is accurate.

The exploitation of savings and loan associations

2020 saw an increase in money laundering problems related to savings and loan associations (S&Ls), increased, whereby the funds collected from the members of the cooperative were transferred out of the cooperative through companies related to the members of the supervisory board or the management board. Companies associated with the members of the management body had often not submit reports for the last few years, there was no actual financial activity and the legal entities were handed over to dummy companies. There were three main objectives for misusing the association: 1) tax evasion; 2) earning personal profits by selling a fictitious service above the market price; 3) misappropriating the assets collected from investors and using them for one's own purposes.

Example 1.

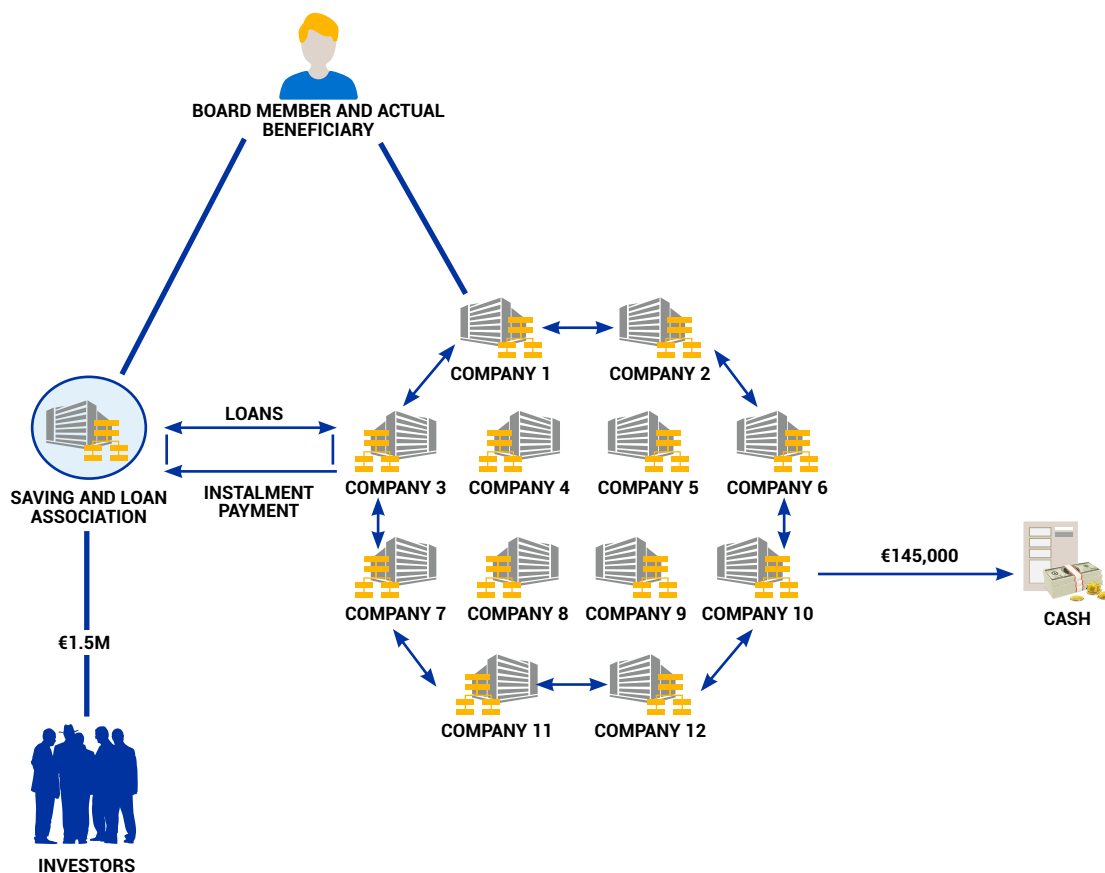
Based on a loan agreement, €120,000 was transferred from S&L X to company No. 1 with ties to a member of the S&L's board. Of this amount, € 70 000 was transferred to company no. 2, also owned by the board member. €117,000 in cash were withdrawn from the first and second companies, after which the companies were re-registered in the name of a foreign dummy company. As companies do not have any actual business activities, the scheme involves moving the money through several companies and thereby avoiding paying taxes.



Scheme 3. Example of using loans and saving associations in criminal schemes

Example 2.

Investors invested €1.5 million into S&L Z. In a series of carousel transactions, the amount received was transferred to one or more parties in order to conceal the origins of the actual assets. The participants in the scheme were dummy companies associated with the savings and loan association and a member of its management board, which had no real economic activity. In order to keep the money constantly moving, the amounts were transferred between the accounts of the parties to the scheme on the same day as they were received. The circulating money, which originally came from the savings and loan association, was transferred in the same amount to the next dummy company, and from there to the next one, and finally returned to the S&L. If, throughout the scheme, the transactions made reference to a loan agreement, then some of repayments to the savings and loan association were explained as "association instalment payments". In order to cover transfer fees, purchase various amenities (including cars or housing), and withdraw cash from ATMs, the dummy companies withheld a few euros to €10,000 at a time from some of the received amounts.



Scheme 4. Example of using loans and saving associations in criminal schemes



5. INTERNATIONAL FINANCIAL SANCTIONS

2020 was a busy year for the FIU as it fulfilled its task of implementing international financial sanctions. Sanctions were imposed in several cases, of which, the case of the Russian media group MIA Rossiya Segodnya continued to attract a great deal of attention among the public.

The FIU's role in international financial sanctions can be conditionally divided into two:

- 1) to organise state supervision of the implementation of financial sanctions in compliance with the requirements of the International Sanctions Act;
- 2) if sanctions are placed on a market participant, to verify the legality of the measures taken by the market participant after receipt of the notification.

Pursuant to §16 (2) of the International Sanctions Act, the FIU provides an annual summary overview of the application of financial sanctions on the identified subjects of financial sanctions, the applied financial sanctions and the granting of allowable exemptions or authorisations. Information on international financial sanctions is provided in table 7.

Table 7. The implementation of financial sanctions in 2020.

Sanctioned person, related person	Measures taken	Date of the measures	Amount in EUR	Exception	Comments
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	7 February 2020	€25,920.38	yes	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	4 March 2020	€5,110.12	yes	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	31 March 2020	€5357.76	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	6 May 2020	€5,623.00	yes	Making financial instruments unavailable
Sergei Viktorovich Chemezov, VSMPO-AVISMA Corporation	frozen	27 April 2020	€2,128.99	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	12 June 2020		no	The Estonian Internet Foundation prohibited the transfer of domain names registered to MIA Rossiya Segodnya. The access to the domain names is restricted.
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	13 June 2020	€12,000	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	3 July 2020	€5,075.84	yes	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	5 August 2020	€5,552.66	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	2 September 2020	€5,539.09	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	2 October 2020	€5,403.97	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	12 October 2020	€218.00	no	Making financial instruments unavailable
Dmitry Konstantinovich Kiselyov, MIA Rossiya Segodnya	frozen	29 October 2020	€15,747.52	no	Making financial instruments unavailable

For the FIU, the cases related to MIA Rossiya Segodnya were largest cases in the course of which international financial sanctions were applied. The measures that were taken are based on the activities of companies related to persons sanctioned by the sanction regime established by European Union Regulation No. 269/2014. This is a quite an old case, which the FIU already introduced in its 2015 and 2019 yearbooks.

The case of application of international financial sanctions against the VSMO-AVSNA Corporation and Sergei Viktorovich Chemezov is based on the activities of companies related to persons sanctioned by the sanction regime established by European Union Regulation No. 269/2014. In 2014, Chemezov was included in the EU's sanctions lists due to its activities that undermine or threaten Ukraine's territorial integrity, sovereignty and independence. The sanctions imposed on Chemezov extend to the legal entities under its control, including the VSMO-AVSNA Corporation. The Estonian credit institution identified a link between the VSMO-AVSNA Corporation and Sergei Viktorovich Chemezov and imposed a financial sanction on the company, and the funds in the account were frozen.



6. LOOKING AHEAD TO 2021

In 2021, several important developments are expected in the Estonian money laundering and terrorist financing system. The Financial Intelligence Unit began 2021 as a new independent institution. An opportunity to improve the prevention of money laundering and terrorist financing has been created, as the FIU is now under the administration of the Ministry responsible for the prevention of money laundering and has been given additional resources to carry out its tasks. An additional expectation for the new FIU is the development of operating principles for and launch of the Strategic Analysis Centre, and a better structure for prevention measures. The current challenge for the FIU continues to be to work simultaneously on building the agency's infrastructure and doing the substantive work in the best possible way.

Estonia will face the following two important international evaluations in 2021: assessment of the effectiveness of the implementation of the Fourth European Union Directive on the Prevention of Money Laundering and Terrorist Financing and the fifth-round assessment of Moneyval compliance and performance. An evaluation of the implementation of the 4th Directive will be carried out by the European Commission in the spring of 2021. An on-site visit by Moneyval evaluators is planned for early 2022, but most of the preparations will take place in 2021. The FIU started preparations in January of 2021.

In the first half of 2021, Estonia's national money laundering and terrorist financing risk assessment (NRA) will be completed, in the implementation of which the FIU, among other institutions, undoubtedly plays an important role. We hope that the NRA provides a good understanding of the risks associated with money laundering, terrorist financing and the proliferation of weapons of mass destruction and as a result of the implementation of the action plan, we are able to properly manage the risks related to all three threats in Estonia.

At the end of 2020, US technical assistance project was started in Estonia, whereby experts from the US Treasury Department are helping to analyse the functioning of the anti-money laundering system as a whole, and among other things, for the FIU to develop strategic analysis capabilities and enhance risk-based supervision. The project has started well and the exchange of experiences has been very useful.

On 5 January 2021, the Ministry of Finance submitted draft legislation related to mutual funds and other investment instruments and virtual currencies. The main objective of the draft legislation is to regulate the provision of co-financing, investment instruments and virtual currencies in a way that mitigates the

risks of money laundering and terrorist financing in the respective areas of activity. Since 2017, the FIU have issued authorisations and supervised virtual currency service providers. Oversight by the FIU is limited to the monitoring of compliance with the requirements of the Money Laundering and Terrorist Financing Prevention Act and does not include financial supervision more broadly. Virtual currency service providers offer a service that is on an equal legal footing with financial institutions and the services are similar in practice. Therefore, it is appropriate that in order to increase the rights of clients in the respective sector as well as the transparency and reliability of the Estonian economic system, the supervision of both virtual currency service providers and co-financing and investment instruments should be extended. According to the draft legislation, supervision would be conducted by the Financial Supervision Authority, which also supervises credit institutions and other main financial institutions. The proposed draft legislation will hopefully enter into force this year. The proposed changes in supervision would significantly reduce the risks of Estonia being used for money laundering and terrorist financing.

During the Covid-19 pandemic, greater use was made of virtual services, as this was sometimes the only way to communicate due to restrictions on movement and reduced physical contacts. However, this increased and expanded cyber fraud, as criminals exploited this important health risk and fear of disease. Finding smart and fast ways to prevent financial crime will continue to be a major challenge for companies intermediating financial transactions in 2021 and to thereby also prevent money laundering. Fast payment solutions are perfectly suited to promoting a daily legal economy, but they can also be misused for criminal purposes. All those who make virtual asset transactions should exercise due diligence in this regard.

In a world of limited resources, the day-to-day use of a risk-based approach is important for all those responsible for combating money laundering and terrorist financing, including the FIU. Therefore, this year the FIU expects to receive support and recommendations from the national risk assessment in order to better target its own monitoring and analysis activities. Various intelligent IT solutions, more of which we want to in the new FIU, will also help to substantially improve our risk-based approach.

We hope to receive comprehensive and meaningful cooperation and support from the new government, which took office at the beginning of 2021, in order to maintain a balance between managing the risks of money laundering and terrorist financing and the needs of business development and promotion. It is certainly not helpful if the system is skewed or unreasonably burdensome for one side or the other. This can be prevented by the availability of the necessary information, its faster and more meaningful analysis, as well as IT solutions, which make information imperceptible to a single pair of eyes more understandable and readable. In terms of resources, smart IT solutions initially require a greater commitment, but this is indispensable in today's information world in order for the new FIU to function effectively as well as for Estonia to become an international trailblazer in the fight against money laundering and terrorist financing.