FINANCIAL INTELLIGENCE UNIT YEARBOOK 2018

OVERVIEW OF THE FINANCIAL INTELLIGENCE UNIT ACTIVITIES IN 2018

TALLINN 2019

CONTENTS

FOREWORD

DEAR READER OF THE FINANCIAL INTELLIGENCE UNIT YEARBOOK

In 2018, serious problems with preventing money laundering in the banks of different member states gradually gained attention and became the most important issue in both the European Union and Estonian anti-money laundering system.

In the light of the occurred money laundering cases, the government committee for the prevention of money laundering and terrorist financing (the AML/CFT Committee) analysed the possibilities of strengthening the Estonian anti-money laundering system. In this yearbook, we introduce the Financial Intelligence Unit (FIU) general perception of what has taken place and reflect some important changes that need to be made in the AML system.

Once again we received several reports on terrorist attacks in European countries in 2018. Although the number of terrorist attacks in Europe show a downward trend, it is still important for all countries in our region to identify payments relating to terrorist financing in the use of foreign fighters returning from conflict zones, individuals at risk of radicalisation and international financial services used to finance the activities of terrorist groups under the cover of legal economic transactions.

One of the major risks that emerged in 2018 for the Financial Intelligence Unit, was the surge in the number of virtual currency providers and the associated risks. We are going to explain our understanding of the need to change existing regulations in detail.

Compliance with the new Money Laundering and Terrorist Financing Prevention Act that entered into force in late autumn of 2017, including the practical implementation of the changes introduced by the European Union Directive on the Prevention of Money Laundering and Terrorist Financing, has been one of the most important issues for obliged entities and state agencies both last year and this year. Many of the cases which attracted media attention show that in the field of attaching more importance to the prevention of money laundering, Estonian service providers still have a room for improvement in focusing on crucial things and leaving irrelevant ones aside through a risk-based approach. However, our society probably needs more time and practice to get used to the fact that, for instance, questions about the origin of the money used in economic transactions or the activities of the business partners asked by a bank or a notary are becoming part of the normal and routine financial hygiene.

Money laundering and terrorist financing are global challenges. The Financial Intelligence Unit is involved in two international networks, the Egmont Group and the FIU.net data exchange platform of the European Union. We are proud of our contribution and the effectiveness of

our international cooperation. Last year we were able to help several foreign partners with valuable information. It is also significant that besides the usual exchange of information between the FIUs, we have established more contact with foreign investigative bodies as well as financial supervisory authorities. Both domestic and international cooperation and exchange of information between the FIUs and investigative bodies, on the one hand, and financial supervision and anti-money laundering supervisory authorities, on the other hand, is one of the keys for increased risk perception and a stronger money laundering and terrorist financing prevention system.

Cases involving exploitation of email accounts and sending fake invoices continued last year. We describe some schemes by which Estonian residents have been cheated out of their money in the cyberworld and how unsuspecting job seekers have been used in international money laundering schemes. We also reflect how suspicious cash flows have mixed with cash flows from legitimate businesses. The following chapters of this yearbook provide a closer look at these and other topics.

On July 1, 2019, the Financial Intelligence Unit celebrates its 20th anniversary. Therefore, we also cover the FIU's activities of the previous years.

Madis Reimand
Head of the Financial Intelligence Unit

1. 20 YEARS OF THE FINANCIAL INTELLIGENCE UNIT

July 1, 1999	the Financial Intelligence Unit (FIU) is established, Arnold Tenusaar becomes the Head of the FIU, Money Laundering Prevention Act enters into force
January 2000	MONEYVAL's first round assessment visit takes place
2000	working group for the prevention of money laundering is created under the Estonian Banking Association
May 16, 2000	the FIU becomes a member of the Egmont Group
March 18, 2000	an inter-agency coordination committee for the prevention of money laundering is established under the Ministry of Internal Affairs
January 1, 2002	the Financial Supervision Authority is established by unifying the Banking Supervision of Eesti Pank, the Insurance Supervisory Authority and Securities Inspectorate working under the Ministry of Finance
November 2002	MONEYVAL's second round assessment visit takes place
January 1, 2004	a thoroughly amended Money Laundering and Terrorist Financing Prevention Act enters into force, the FIU's staff is increased to 8 employees
August 9, 2004	Raul Vahtra becomes the Head of the FIU
May 11, 2006	the government committee for the prevention of money laundering (the AML/CFT Committee) and the council of market participants are established at the Ministry of Finance
March 1, 2007	the Asset Recovery Office is established at the FIU
January 1, 2008	a new Money Laundering and Terrorist Financing Prevention Act enters into force, the FIU gets a new information system called RABIS
February 2008	MONEYVAL's third round assessment visit takes place
January 1, 2010	the FIU's Asset Recovery Office becomes an independent bureau
January 22, 2010	Payment Institutions and E-money Institutions Act enters into force
January 2, 2013	Aivar Paul becomes the Head of the FIU
November 2013	MONEYVAL's fourth round assessment visit takes place
April 1, 2016	Madis Reimand becomes the Head of the FIU
November 26, 2017	a thoroughly amended Money Laundering and Terrorist Financing Prevention Act enters into force

July 1, 1999 can be considered to be the starting point of the anti-money laundering system in Estonia, as two events of considerable significance took place: the Financial Intelligence Unit (FIU) was established and the Money Laundering Prevention Act entered into force. The first Head of the FIU was Arnold Tenusaar.

Less than a year later, on May 16, 2000, Estonia became a member of the Egmont Group. This was a great recognition and a sign that Estonia's anti-money laundering system had international credibility.

The first decade of the new millennium saw the establishment of a number of institutions and networks still playing an important role in the anti-money laundering system: an inter-agency coordination committee and a working group for the prevention of money laundering under the Estonian Banking Association in 2000, the Financial Supervision Authority in 2002, the government committee for the prevention of money laundering and the council of market participants in 2006. The main task of the latter was to raise the entrepreneurs' awareness of the prevention of money laundering and terrorist financing and to give them the opportunity to contribute to the drafting of legislation related to money laundering and terrorist financing. The council is made up of employees of the Ministry of Finance, along with representatives of various business associations and other relevant agencies.

In January 2000, MONEYVAL's[1] first round evaluation took place in Estonia. Evaluation experts found that although Estonia had taken important steps to prevent money laundering – for instance, the Money Laundering Prevention Act had been passed, the obligation to report suspicious transactions had been introduced, the FIU had been established – there were also a number of bottlenecks in the system, such as the definition of money laundering being too narrow, no possibility to hold legal persons liable for money laundering, confiscation being possible only in a few cases, etc.

In November 2002, MONEYVAL's second round evaluation took place in Estonia. Evaluators found that a system where money laundering proceedings can be initiated without a conviction for a predicate offence already in force, but where a conviction for money laundering must be preceded by a conviction for a predicate offence, is problematic. It was also pointed out that the possibilities for confiscation should be extended and be mandatory for money laundering offences. In addition, it was found that the FIU's resources should be boosted in order to increase the capacity for analysing incoming reports and sending them into investigation. Estonia's progress in the prevention of money laundering, including adding a supervisory task to the Financial Supervision Authority established in January 2002 and the licensing of credit and financial institutions by the Financial Supervision Authority, was deemed positive. It was also pointed out that Estonia had ratified the Strasbourg Convention and the Vienna Convention.

In January 2004, a thoroughly revised law, bearing the name Money Laundering and Terrorist Financing Prevention Act, came into force. Regulation on terrorist financing was added to the law. In order to prevent money laundering and terrorist financing, credit and financial institutions were now obliged to check their customers on the basis of given lists. The subjects of the Act were expanded to meet the requirements of the second EU Money Laundering Directive, and foreign exchange services and money transfer service providers, attorneys, notaries, auditors and tax advisors were added to the list of obliged entities. Currency exchange service providers were now obliged to register their businesses. The FIU's role also changed: a supervisory function was added to it. The FIU gained the right to issue administrative decisions, inter alia to suspend transactions for up to two business days and to seize property for up to 10 business days.

[1] MONEYVAL (the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism) is an expert committee of the Council of Europe engaged in the fight against money laundering and terrorist financing. MONEYVAL (formerly PC-R-EV) was established in 1997 by the Committee of Ministers of the Council of Europe to assess its members' compliance with anti-money laundering measures implemented in those member states of the Council of Europe that are not members of the FATF (the Financial Action Task Force is an intergovernmental organisation of democratic nations that issues standards and methods to combat money laundering and terrorist financing, and promotes policies in this area).

In January 2008, the new Money Laundering and Terrorist Financing Prevention Act came into force, by which the principles arising from the third anti-money laundering directive 2005/60/EC were transposed into Estonian legal system. Situations in which the institutions or persons covered by the directive have to identify the customer and verify their identity were now governed more accurately. In most cases, the existing verifications made by credit institutions could be relied upon, but financial service providers had to meet their customer face to face at least for the first time before establishing a business relationship. As a new requirement, the obliged entities, except credit institutions, had to report any transactions involving 500,000 kroons in cash or other currencies to the FIU. Credit institutions were obligated to report only if they were acting as currency exchange offices. All financial service providers who did not fall under the supervision of the Financial Supervision Authority had to register at the Register of Economic Activities. Requirements for individuals who could serve as members of the management bodies of such companies were specified precisely. They could register on the condition that they had no current criminal punishments for intentionally committed crimes or crimes related to money laundering or terrorist financing.

In February 2008, MONEYVAL's third round evaluation took place in Estonia. This evaluation recognized the steps Estonia had taken and pointed out that Estonia had a suitable legal and institutional environment for preventing money laundering and terrorist financing. One of the major shortcomings noted was the fact that there was no possibility of prosecuting individuals liable for terrorist financing in Estonia.

In January 2010, Payment Institutions and E-money Institutions Act entered into force, by which financial service providers were now obliged to apply for the Financial Supervision Authority's authorisation.

In November 2013, MONEYVAL's fourth round evaluation took place in Estonia. The evaluation report listed that Estonia had strengthened its system to prevent money laundering and terrorist financing, the Money Laundering and Terrorist Financing Prevention Act included a risk-based approach, and the obligations to „know your customer," keep records and report were largely in line with the recommendations of FATF. The report also recognised, as areas for further improvement, the system for identifying the beneficial owner, and the absence of a legal framework to regulate the monitoring of unusually large transactions and transactions between persons from countries that do not follow the FATF recommendations or do it inadequately. In addition, the existing sanctioning system needed improvements, as the penalties that the Financial Supervision Authority and the FIU could impose were very low.

In November 2017, a thoroughly amended Money Laundering and Terrorist Financing Prevention Act entered into force. It brought Estonian legislation into conformity with the new international standards for anti-money laundering measures and combating the financing of terrorism issued by the FATF in 2012. Also, the fourth anti-money laundering directive was transposed and some changes regarding the fifth anti-money laundering directive were introduced. The scope of the Act was extended and a risk-based approach incorporated into Estonian law. The Act set an obligation for companies to submit the data of beneficial owners to the commercial register. The list of obliged entities now included providers of virtual currency exchange services and virtual currency wallet services, as well as undertakings providing a cross-border cash and securities transportation service. Terms of punishment were harmonised and the maximum punishment for the misdemeanour of violating the requirements of the Money Laundering and Terrorist Financing Prevention Act was increased up to 400,000 euros.

The FIU was established on July 1, 1999 and will celebrate its 20th anniversary on July 1, 2019. The FIU's duties have expanded over time but the main tasks since its establishment have been collecting and analysing information on transactions with suspicion of money laundering and terrorist financing, and in case a suspicion of crime has been identified, forwarding this information for deciding whether a pre-trial investigation should be initiated. The FIU receives reports by all entities who have or may have contact with potential money laundering, i.e. banks and payment institutions within the financial sector but also many others, such as notaries, attorneys and auditors.

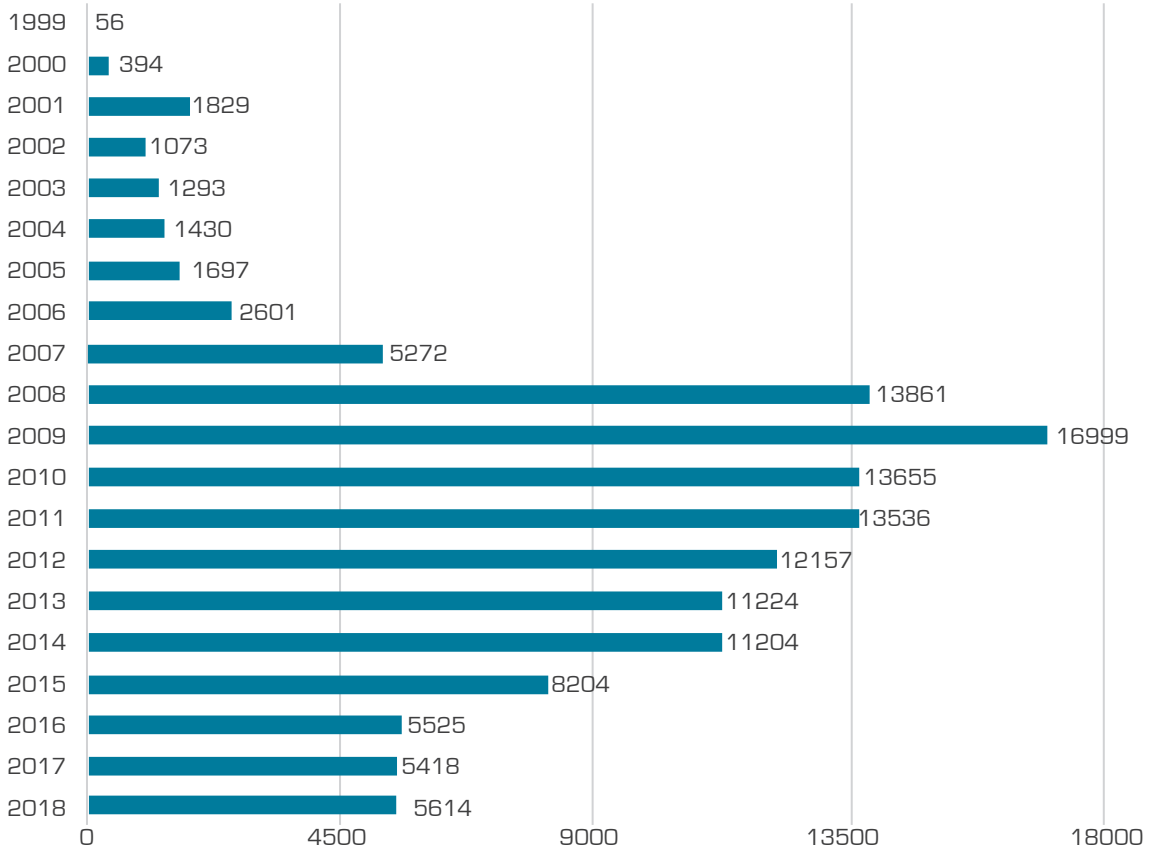


Figure 1. The number of reports received by the FIU between 1999-2018

The Financial Intelligence Unit performs a unique task because, under certain conditions, persons ordinarily obliged to maintain the confidentiality of their customers take the initiative to inform the FIU of certain customers and transactions, even if the information provided is subject to banking secrecy. The FIU maintains the confidentiality of the information it receives and only forwards information needed to prevent, identify and investigate crimes to investigative bodies, the Prosecutor's Office and the court. The investigative bodies and the Prosecutor's Office identify money laundering in pending criminal cases, while the FIU identifies possible money laundering incidents on the basis of financial information from the private sector.

During its 19.5 years of operation (from July 1, 1999 to December 31, 2018), the FIU has received 133,042 reports. Figure 1 shows the extent to which the number of reports received by the FIU has varied: in the first year, the FIU received 56 reports. The number of reports reached its peak in 2009, when the FIU received 16,999 reports. In recent years, the number has remained around 5400-5600.

The FIU has other tasks as well that support the achievement of the aforementioned key objectives. If necessary, the FIU can impose restrictions on the use of property. The Money Laundering and Terrorist Financing Prevention Act is enforced by the Financial Intelligence Unit in regard to obliged entities and by the Financial Supervision Authority in regard to persons who have been granted their authorisation, as well as by the Estonian Bar Association and the

Chamber of Notaries in regard to their members (supervision over notaries is delegated by the Ministry of Justice to the Chamber of Notaries). The FIU also supervises compliance with the requirements pertaining to financial sanctions imposed under the International Sanctions Act. In the case of international financial sanctions, the Financial Intelligence Unit acts as the central unit that coordinates and supervises the implementation of relevant sanctions, imposes restrictions on the use of funds and assets, if necessary, and in circumstances of exceptional necessity, issues permits to perform transactions subject to sanctions.

The Financial Intelligence Unit also issues authorisations. These include authorisations for financial institutions that have not been granted an authorisation by the Financial Supervision Authority, as well as authorisations for providers of trust and company services, providers of a service of exchanging a virtual currency against a fiat currency and providers of a virtual currency wallet service, pawnbrokers, and persons engaged in buying-in or wholesale of precious metals and precious stones. The functions of the Financial Intelligence Unit also include tracing criminal proceeds, cooperating with investigative authorities, the Prosecutor's Office and foreign financial intelligence units, strategically analysing the trends and threats of money laundering and terrorist financing, and notifying the public.

During its 20 years of operation, the Financial Intelligence Unit has had four Heads. We asked the former Heads of the FIU to answer four questions.

1. What was the greatest challenge you had to face while working at the FIU?
2. What was your greatest achievement at the FIU?
3. What is the most important issue to be resolved in the Estonian anti-money laundering system?
4. What makes you proud of the FIU?

ARNOLD TENUSAAR, HEAD OF THE FIU 1999–2004

When I was appointed Head of the FIU in June 1999, it wasn't the first time I had received a task of stepping into the unknown and doing things I had never done before. I had been in the same situation seven years earlier when I had to start building the Interpol National Central Bureau from scratch. But perhaps my previous successful experience was the reason for my appointment. Once again, I had to start from myself and then begin explaining new concepts and new principles that did not exactly match the previous ones to other participants of this project. It took five years from the enforcement of the Money Laundering Prevention Act to securing a conviction for money laundering, which clearly illustrates the slow pace of setting up the system. However, we weren't any slower in comparison with other countries. Nevertheless, this wasn't my biggest challenge at the FIU.

The anti-money laundering system is based on trust. Therefore, the hardest task was to win the trust of market participants so they would report suspicious transactions, while being confident that the use of this sensitive information would be limited solely to the cases and according to the procedures laid down by law. On the one hand, gaining trust became challenging because of the FIU's low position in the structure of the Estonian Police. It was difficult to convey the FIU's statutory independence in this structure credibly. On the other hand, there were colleagues in the police force who thought of facilitating their work by using the authority of the FIU in gaining an easier access to the bank accounts of interest. We managed to overcome this challenge and win the trust of market participants, as well as protect our independence in the police structure. This was my greatest achievement at the FIU.

We have been building and developing our anti-money laundering system for almost 20 years. The cases of Danske and Verso highlighted that not all financial market participants considered it important to

exercise due diligence and, blinded by profit, allowed suspicious transactions to take place and failed to inform us about them. While investigating the cases, it had to be acknowledged that the whole system from the obliged entities and the FIU to the investigative authorities were underfunded and thus undermanned. There was neither knowledge or experience, nor any legal means to control the transit of such large cash flows of unknown origin. In addition, there was no mechanism for strategic analysis that would have issued a timely warning on the basis of economic indicators. Let us hope that the policymakers will assess the real situation properly and take adequate measures to adopt necessary amendments so that required resources could be provided to law enforcement and supervisory authorities and the transit of suspicious cash flows could be controlled.

RAUL VAHTRA, HEAD OF THE FIU 2004-2012

To sum up, the main areas I focused on (and managed to implement) while being the Head of the FIU were the following:

1) Increasing the administrative capacity of the FIU;
2) Developing a new information system (RABIS) for the FIU + creating the opportunity to report suspicious transactions electronically;
3) Creating the capacity to supervise obliged entities within the FIU;
4) Creating the capacity to identify criminal proceeds within the Estonian Police;
5) Active prevention (raising awareness of money laundering and terrorist financing among law enforcement agencies and obliged entities);
6) Putting the FIU on the international map (cooperation agreements with other FIUs, active participation in various international projects and organisations).

When I started working at the Financial Intelligence Unit in 2004, my biggest challenge was to turn the FIU into a professional unit with administrative capacity and good reputation both in Estonia and abroad. It was a period when numerous changes took place in the area of money laundering. In 2001, the European Parliament and the Council adopted the second money laundering directive, the principles of which had to be incorporated into Estonian law. The second major challenge was to increase the administrative capacity of the FIU. In addition, the FIU did not have a modern database. Reports of suspicious transactions were largely received on paper and it became clear that this would not be sustainable in the long run. In addition, it was time to get serious about raising awareness of anti-money laundering among law enforcement agencies as well as obliged entities. In order to do it, we filed an application to the European Union PHARE programme and received funding for the project. In 2005, we started the EU Twinning project "Integrated programme to strengthen the capacity of the Estonian anti-money laundering institutions" (2004/006-270.04.03). We collaborated with the Dutch FIU and together managed to set up a modern information system for our FIU. In addition, we conducted numerous trainings for obliged entities, supervisory and investigative authorities, prosecutors and judges. I believe this was the turning point, when people started to take anti-money laundering seriously in Estonia. The number of reports the FIU received on suspicious transactions increased significantly.

Another major challenge was to establish the capacity to trace criminal proceeds in Estonia. We started with these activities in 2006 and relied on the Council document 15628/05 ADD 1 of 14 December 2005, which stated that the European Commission encourages member states to set up Criminal Asset Intelligence Units. Article 1 obliged each member state to set up or designate a national Asset Recovery Office.

I introduced this idea to the Police administration of that time and proposed to create the capacity to trace criminal proceeds within the Financial Intelligence Unit and to set up a separate Asset Recovery Division to serve this purpose. The Police administration agreed with the proposal. In 2006, the Financial Intelligence Unit prepared for the launch of a new twinning project to support the creation of a National Monitoring Centre of criminal proceeds and to make fighting against criminal proceeds more effective. In 2007, the project was launched in collaboration with the German Berlin Police. The project proved to be very successful. We trained a number of law enforcement employees, prosecutors and judges in the area of criminal proceeds. An Asset Recovery Division comprised of five trained officials became operational under the Financial Intelligence Unit. The project ended in 2009. Later, the Asset Recovery Division became a separate Asset Recovery Bureau and I am pleased to note that identifying criminal proceeds has now become a natural part of proceedings.

In 2008, a new Money Laundering and Terrorist Financing Prevention Act came into force. This meant widespread changes in the anti-money laundering system and, at the same time, it introduced an obligation to start preventing terrorist financing in addition to money laundering. It also regarded international sanctions. New supervised entities were added as well. It was all a very new and exciting challenge for us, and in cooperation with state agencies and financial institutions we managed to make the system operational. The period between 2008-2012 was extremely busy. Certain new trends appeared in money laundering (the so-called Russian Laundromat) and the number of reports on suspicious transactions reached an all-time high. As we now know, transactions that have become public in connection with the Danske Bank money laundering scandal, also took place during that period.

In conclusion, I really enjoyed working at the FIU. We managed to achieve some great things. The team was fantastic and together we were in close cooperation with the regulators of the Ministry of Finance. It was great to see enthusiastic people happily doing their job. However, some things still bothered me. We would have expected criminal proceedings to be commenced more boldly and brought before court in case of ownerless money of suspicious origin. Even negative court decisions would have been a way forward, as we would have got a better idea of legal possibilities and been able to change them, if necessary. The same problem still exists. I remain hopeful that one day we would reach a point, where money without an owner or of unknown origin did not move through Estonia's financial system or its economy, and if it did, the state would have the opportunity to confiscate it. This is the only way of making sure that money launderers would not risk making transactions through Estonia.

AIVAR PAUL, HEAD OF THE FIU 2013-2016

I started working at the Financial Intelligence Unit on its first day of operation on July 1, 1999. I headed to the FIU from the investigation department of the Central Criminal Police at the invitation of Arnold Tenusaar, the first Head of the FIU. After a couple of years of helping to set the anti-money laundering going at the FIU, I headed to the private sector. Yet a part of me remained with the Police and the Financial Intelligence Unit. I returned to the FIU as its Head at the beginning of 2013, when both Estonia and the FIU were facing several important challenges that had to be overcome.

One of those challenges was a previous decision that the FIU would start issuing authorisations to those subjects of the Money Laundering and Terrorist Financing Prevention Act, who were not under the supervision of the Financial Supervision Authority. This

meant a change to the concept of the existing registration system and, unfortunately, a very limited change at that, since the only grounds for refusal was a previous punishment.

Another challenge was to prepare and participate in a national money laundering risk assessment. The risk assessment, which was based on the World Bank risk assessment methodology, was finalised in 2015. It was the first document of its kind for Estonia and all agencies and private sector representatives were involved in the process. Within the framework of this project, we assessed every possible field of activity concerning money laundering by way of all processes and procedural steps. I should add that it was perhaps one of the biggest awareness-raising projects on anti-money laundering.

The third challenge was MONEYVAL's evaluation, or the assessment of the state as a whole according to the FATF recommendations. The assessment process is always an extremely resource-intensive exercise, while its results have a considerable impact on the reputation of Estonia. We managed to defend Estonia's report of 2014 with very good results.

Furthermore, securing funding for the FIU's new information system and preparing the first strategic analyses may also be seen as challenges.

Unfortunately, not everything goes as planned. So, for instance, the realisation that the possibility of entering ownerless property into public revenues under the Money Laundering and Terrorist Financing Prevention Act could not be used in practice was a bitter pill to swallow. This was due to a decision of the Supreme Court, not related to money laundering, that essentially defined the assets in a bank account as a right of claim against the bank. These assets always belong to the account holder, irrespective of the way in which they were received. Examples include a case, in which a front man confirmed to the court that the money in his account was not his and he did not want it. However, the judge, following the precedent of the Supreme Court, made a judgment that this money could not be taken into public revenues because it had an owner, meaning the account had a holder. This precedent made it impossible to use the opportunity given by the Money Laundering and Terrorist Financing Prevention Act in cases like this. At the moment, there is an initiative to reintroduce a similar possibility by implementing reversed burden of proof.

Also, I'm disturbed by the acquittal of the accused in one of the biggest money laundering cases, although the court essentially confirmed the proof of concealment (the use of front men, filing fictional and falsified documents, giving false testimonies etc.). However, since it was not possible to get proof of predicate offence from the original state, Russia, the case was acquitted. In this respect, I would like to thank the State Prosecutor, who made some great efforts to get a fair judgment for this case, by trying to make the most of the possibilities of the judicial area of that time.

Active exchange of information with the Financial Supervision Authority illustrates a positive example of cooperation. As a result, the Financial Supervision Authority issued a legal instrument regarding a bank that is now at the centre of the largest money laundering scandal in Estonia. Since the FIU's main task is to serve as a filter that analyses reports on suspected money laundering received from the private sector and forwards them for investigation, the FIU's information is limited to what it receives. Uncovering of this case began slowly with individual queries sent from Moldova, Ukraine and other countries, and finally grew into a large-scale network. However, the information concerning the total possible volume of the schemes later published by the media came as a negative surprise.

2. THE YEAR 2018 IN THE ESTONIAN ANTI-MONEY LAUNDERING SYSTEM

2.1. MONEY LAUNDERING RISKS OF THE FINANCIAL SYSTEM

In 2018, a number of money laundering incidents and suspicions related to banks were under scrutiny in Europe. Let us mention some of them: problems and pending criminal cases against Deutsche Bank, ING Bank in the Netherlands and Danske Bank continued to attract publicity; the European Central Bank shut down Malta's Pilatus Bank, the ABLV Bank in Latvia went into liquidation due to public accusations of money laundering, etc. The year 2019 has added the so-called Troika Laundromat in which Lithuania's Ukio Bankas, that was closed a few years ago, had its role to play, and that has connections to many large banks, including the Danske Bank, the Austrian Raiffeisen Bank and the French Credit Agricole Bank. In addition, there are references to suspicious cash flows in the Swedish banks Nordea and Swedbank.

These cases clearly demonstrate that the financial markets have become globalised and money laundering is a problem that does not respect any national borders and is not isolated to a single bank, state or financial system. This has to be taken into account when supervising anti-money laundering, exchanging information, or investigating crime.

The year 2018 in the Estonian anti-money laundering system took off with a report that the European Central Bank would revoke the licence of Versobank over failures to remedy regulatory breaches in money laundering. The year ended with a report issued by the Central Criminal Police and the Prosecutor's Office on the detention of ten former employees of Danske Bank on suspicion of money laundering. The case of Danske Bank gained the centre of attention and raised some questions about the incident and the functioning of the Estonian anti-money laundering system, to which the media, the public, obliged entities and state institutions tried to find answers. Considering the fact that the criminal proceedings that were commenced based on a report of a criminal offence submitted by the Financial Intelligence Unit in November 2017 are still in the phase of pre-trial proceedings, we are not in a position to disclose any information concerning the investigation. However, we try to explain some of the aspects of what has happened from the FIU's point of view.

2.1.1. Reducing risks in the Estonian financial system

Both the Financial Supervision Authority and the Financial Intelligence Unit have previously confirmed that money laundering risks related to large-scale cross-border transactions have decreased significantly in recent years. The reduction of risks can be illustrated by the fact that FIU sees far less of such cases and the amounts concerned are significantly smaller than in some previous larger cases (you can read about the four major money laundering schemes identified by the FIU from the previous yearbook[2]). The fact that several important actors in the banking sector have been mitigating anti-money laundering risks is also reflected in the number of reports received by the FIU. Between 2016 and the end of 2018, banks have sent more than 1,800 reports on ending customer relationships due to suspicion of money laundering or the fact that it was not possible to obtain sufficient information on customer's activities in the course of due diligence measures. This indicator rose to the forefront of the main reasons for reporting in 2016. On the one hand, the large number of such reports shows the activities of several banks in mitigating risks. On the other hand, these figures reflect that the financial system has had significant risks to mitigate, and customers who made transactions that were risky or suspicios.

We have seen that the level of money laundering risks and the starting time and pace of their mitigation have been different in various Estonian banks and therefore we cannot draw conclusions from the aforementioned assessment about each individual bank operating in the Estonian market. Various participants in the financial system have understood the changes in the anti-money laundering situation, and the need to reassess risks and the ranges of what constitutes permissible and impermissible, during different times and their starting point in accepting previous risks and offering services to non-residents has differed. Consid-

[2] https://www2.politsei.ee/dotAsset/807911.pdf

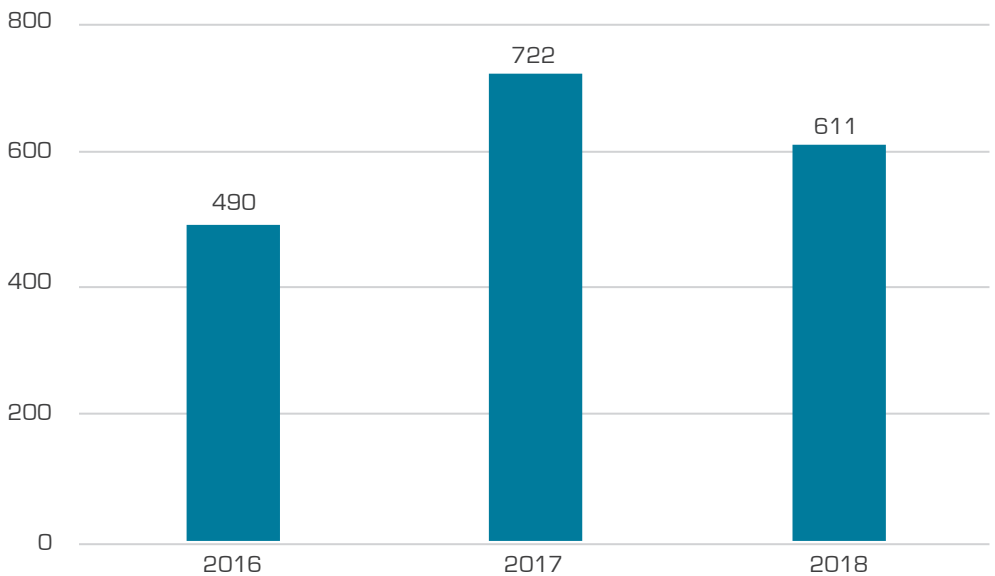


Figure 2. The number of reports received by the FIU, where the indicator set was "A credit or financial institution ends a customer relationship due to suspicion of money laundering or failure to submit documents or relevant information necessary for compliance with due diligence measures."

ering the volume of those suspicious cash-flows related to non-residents that have passed through Estonia and the role the Estonian branch of Danske Bank, Versobank or some other regional banks have played in the Estonian financial system and in clearing with other banks, it is obvious the majority of banks that have provided payment services cannot claim that the transit of suspicious cash-flows has not been of any concern to them. However, the emergence of such links with suspicious transactions by themselves does not necessarily mean that these specific banks had significant or systemic issues with preventing money laundering.

2.1.2. The responsibility of financial institutions and the normal functioning of the anti-money laundering system

Both this year, as well as the last year, the press published several reports on how a number of other credit institutions have received suspicious payments from dubious accounts related to, for instance, Danske Bank. Due to the high profile of the Danske Bank case, questions about the bank's responsibility and its role in allowing suspicious transactions to take place have arisen in almost all of these cases.

In general, we can distinguish three scenarios in the abuse of financial services depending on the functioning of the bank's anti-money laundering system.

In the first case scenario, the level at which the bank's anti-money laundering systems function, due diligence is exercised and transactions are monitored, is sufficient and money laundering risks are well mitigated. Even in this case, it is not possible to exclude the movement of criminal money. This risk can only be mitigated to an optimal level. Conditions have to be created in which the bank can identify a sufficiently large number of problematic transactions before the transactions have been completed and the assets transferred. The reporting obligation of the entire financial system has been built on an understanding that a bank is an important participant in the anti-money laundering system and makes considerable efforts to identify suspicious transactions by the abusers of banking services, and to inform law enforcement authorities via the FIU.

In the second case scenario, the bank makes efforts to exercise due diligence and prevent money laundering, but the measures taken by the bank are not sufficient in terms of risks and need to be stepped up. The bank is an important participant in the anti-money laundering system and makes considerable efforts to identify and prevent suspicious transactions by the abusers of banking services, but these efforts are not sufficient considering the risks. The bank needs to strengthen the anti-money laundering systems or reduce the risks associated with money laundering, for instance by terminating the provision of some services or the provision of services to specific customer groups. In some cases, a financial institution is able to understand that it has reached this level and makes efforts to return to the aforementioned first level. In other cases, supervisory authorities need to direct and prescribe service providers. Upon receiving such instructions, the bank cooperates and contributes to the elimination of shortcomings.

In the third case scenario, the bank's anti-money laundering systems are basically ineffective and inadequate for mitigating money laundering risks. As a rule, the bank does not make any serious efforts to improve the prevention of money laundering or to reduce risks. This could be the case even when a law enforcement or supervisory authority draws attention to the situation. The bank acts as if it was preventing money laundering, exercising due diligence, sending reports, etc. but all of this is done formally and in a manner that does not substantially mitigate the risks or prevent the abuse of financial services. Depending on the financial institution's portfolio of its customers and services, it might prove impossible for some service providers to set up systems that would effectively mitigate taken risks in practice. With some customers, the risks are just so high that the only way to mitigate them effectively is to give up providing services to them. In some cases, the business model of the service provider cannot withstand necessary changes, which makes it impossible to give up servicing high-risk customers. In those cases, only effective application of the enforcement powers of the state can ensure that such service providers are reprimanded and, if necessary, withdrawn from the market. In criminal cases, we cannot

exclude the fact that some service providers may direct their activities towards allowing or even helping their customers to commit crime.

In all cases in which it becomes public that money of suspicious origin or criminal money has passed through a bank, it cannot be assumed that the bank has contributed to this activity or indirectly allowed it to happen through its insufficient anti-money laundering system. In order to make such an assessment in case of large scale cases and suspicions, we must understand which of the three aforementioned levels the financial service provider is at or was at the time the transactions took place. In most cases, publicly available information is not sufficient for making such an assessment. It is necessary to assess information on transactions, associated persons, legal grounds for transactions and documents, as well as information on exercising due diligence, which signs of suspicious activity appeared, if and how they were reacted upon, etc. At a primary level, in case of financial institutions, such assessments can be carried out by a supervisory authority and in case of banks they are carried out by the Financial Supervision Authority. If the circumstances of a case indicate deliberate assistance in criminal activities, then such an assessment can be made by the Prosecutor's Office and investigative bodies during the criminal proceedings. The role of the Financial Intelligence Unit is to be a good partner for both sides and to support them with its gathered information and analyses.

We can confirm that the FIU, the Financial Supervision Authority, the Prosecutor's Office and supervisory bodies have been exchanging such information and assessments for some time. However, these assessments can reach the public somewhat later, when following supervisory procedures, the Financial Supervision Authority has formed an opinion on whether a financial service provider has complied with obligations to prevent money laundering, or when the Prosecutor's Office and investigative bodies have formed an opinion in criminal proceedings concerning some money laundering cases connected to the service provider. Both the Financial Supervision Authority's track record in supervising the prevention of money laundering, and the criminal proceedings initiated in connection with large-scale money laundering cases, provide assurance that state agencies use the aforementioned assessment scale and implement appropriate measures, ranging from drawing attention to weaknesses up to limiting commercial activities, revoking authorisations and bringing charges.

2.2. THE INCREASE IN RISKS RELATED TO VIRTUAL CURRENCIES

One of the major risks that emerged in 2018 for the Financial Intelligence Unit was the explosive growth of virtual currency providers and the increase of associated risks. The new Money Laundering and Terrorist Financing Prevention Act that came into force in the autumn-winter for 2018, as well as the amendments introduced by the EU directive have brought about a significant increase of risks in this area. These risks are related to fraud, money laundering and terrorist financing. The Financial Intelligence Unit has seen signs of how its authorisations in this area could be used to create the necessary trust required for fraudulent activities, to provide services requiring authorisations issued by financial supervision authorities in foreign countries, and to launder money. Furthermore, there are high risks related to criminals making use of service providers' inadequate due diligence measures to transfer criminal money. It is also worrying, that we have seen signs of how foreigners suspected of terrorism have tried to open accounts with Estonian service providers.

Mitigating the risks associated with virtual currencies is not possible merely in the context of norms guided by the aspects of anti-money laundering. As a spokesman for digital technology, Estonia needs to develop policies and the required regulatory environment by taking the broader context into account. In addition to preventing money laundering and terrorist financing, it is necessary to take into account technological development, the credibility of virtual currency providers and the protection of the interests of individuals and companies using their services.

Regulating the field in the context of money laundering

and terrorist financing is not sufficient and we need rapid intervention by policy makers and legislators. Unfortunately, our parliament did not have enough time at the end of its term to discuss and adopt any primary measures to mitigate at least some of the risks. By the time of the publication of this yearbook, Estonian parliament, the Riigikogu, has opened the proceedings on the draft resolution providing primary relief measures. We hope that the new Riigikogu will make fast progress in this respect, so the policymakers would get an opportunity to formulate proposals concerning the development of virtual currency policies and the relevant regulatory framework by looking at the broader picture.

2.3. POSSIBILITIES FOR FURTHER DEVELOPMENT OF THE ESTONIAN ANTI-MONEY LAUNDERING SYSTEM

The government committee for the prevention of money laundering and terrorist financing (the AML/CFT Committee) compiled a report at the request of the government on the lessons of large-scale money laundering cases and set up two expert groups to analyse and strengthen the Estonian money laundering and terrorist financing prevention system. The following paragraphs provide a brief overview of some suggestions from the the AML/CFT Committee and expert committees on how to strengthen the system.

2.3.1. Increasing the capacity for strategic analysis

It is necessary to strengthen the capacity for strategic analysis of money laundering prevention in order to detect the risks of money laundering and terrorist financing early on, to adequately perceive the level of risks involved and to guide activities to mitigate them. There is a need for establishing the process of developing money laundering prevention situational assessment combining nationwide information, defining the task of monitoring incoming cash flows, and setting up an appropriate system. At present, the information concerning money laundering prevention is fragmented amongst various actors. The Financial Intelligence Unit is not entitled to receive the information on banks and the financial sector gathered by the Central Bank of the Republic of Estonia and available to the Financial Supervision Authority in order to assess the risks of money laundering. The Financial Supervision Authority has a right to forward information to the FIU in case of suspicion of money laundering but not, for instance, in order to assess the risk of money laundering or terrorist financing in a particular financial institution or sector. Access to information on cross-border payments is also needed for a regular assessment of the risk situation. In addition to the financial sector, it is also necessary to gather information from other obliged entities who do not currently submit relevant statistical reports, in order to understand the risks of money laundering and terrorist financing in Estonia. For instance, information is needed on the volume and classification of services provided by virtual currency providers, the volume of customers' transactions, the distribution of customer profiles and their customers' residency.

Processing such data together with the information from the FIU and the investigative bodies is a vital prerequisite for understanding the risks to our financial system and for directing the resources and activities of money laundering and terrorist financing authorities to those areas where risks and threats are the highest.

At its meetings of March and April 2019, the AML/CFT Committee approved the establishment of such a strategic function with the FIU, the initiation of necessary activities and the preparation of draft resolutions to amend legislation.

In our opinion, the main conclusions to be drawn from the Danske Bank case to strengthen the anti-money laundering system are that the legal remedies in criminal proceedings have been inefficient over a long period of time and in order to respond to such cases more quickly, we need to establish a situational picture of money laundering prevention combin-

ing nationwide information, define the task of monitoring incoming cash flows and set up an appropriate system. It is also necessary to review the legal instruments and resources available to the participants of the anti-money laundering system

2.3.2. Authorisation procedure, supervisory measures and coercive measures

We have already mentioned the need to strengthen the legal instruments of the FIU's authorisation procedure. We noted in our previous yearbook that one of the components of a functioning system has to be a flexible and rapidly responding supervisory activity armed with strong coercive measures and sufficient resources. Unfortunately, the coercive measures currently in place are unsatisfactory. A fine of only tens or hundreds of thousands of euros does not discourage service providers who could make millions by breaking the anti-money laundering rules. In addition to the amount of fines, the entire process of misdemeanour proceedings needs to be amended, at least what concerns the violation of the anti-money laundering regulation. Either the misdemeanour proceedings need to be amended or an institution of administrative responsibility and administrative fines set up in this area. The current reality in major cases is that a large number of misdemeanours expire during the court proceedings or before the violations are detected. Unfortunately, a violation detected by a service provider is not enough to impose a punishment. It is also necessary to identify the employee of the service provider who is responsible for the violation. However, if the distribution of responsibilities between the employees is unclear, the financial institution that is violating the rules does not have to fear punishment for misdemeanour. These are the issues that need to be tackled.

In the previous yearbook, we discussed thoroughly the difficulties of proving a predicate offence. This has been one of the reasons why the legal remedies in criminal proceedings have been inefficient in tackling the transit of suspicious international transactions. That problem still needs a solution in Estonia. This is why we have proposed reversing the burden of proof with regard to money laundering outside the framework of criminal proceedings. Will the solution be the proposed reverse burden of proof and the possibility of seizing assets in administrative proceedings or should we look toward criminal proceedings to find solutions for changing the standard of proof? Perhaps we should follow the example of Dutch practice, where criminal courts convict criminals of money laundering and seize assets even if a predicate offence is unknown, but there is good reason to believe that in addition to transactions under suspicion of money laundering, the assets are of criminal origin. We expect the discussions ahead to provide an answer to how to solve the failure of proving a predicate offence.

2.3.3. Resources and other issues

One of the main conclusions of the committee was that the resources at the disposal of the key players in the anti-money laundering system need to be upgraded in terms of both human resources and competence building, as well as financing and IT solutions. The first steps have already been taken.

Furthermore, the AML/CFT Committee and its expert groups addressed a number of issues ranging from laying down the elements of specific misdemeanours up to applying specific due diligence measures. We cannot cover all of these issues in this yearbook. However, we can hopefully soon read about most of them from the draft bills.

3. OVERVIEW OF THE PERFORMANCE OF THE FINANCIAL INTELLIGENCE UNIT IN 2018

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

In 2018, the FIU received 5,614 reports (Figure 3), which is on the same level as the number of reports in 2017.

More than three quarters of the reports received in 2018 were suspicion-based and less than one third were cash transaction reports (Figure 4). In recent years, the share of suspicion-based reports has increased year by year: in 2016

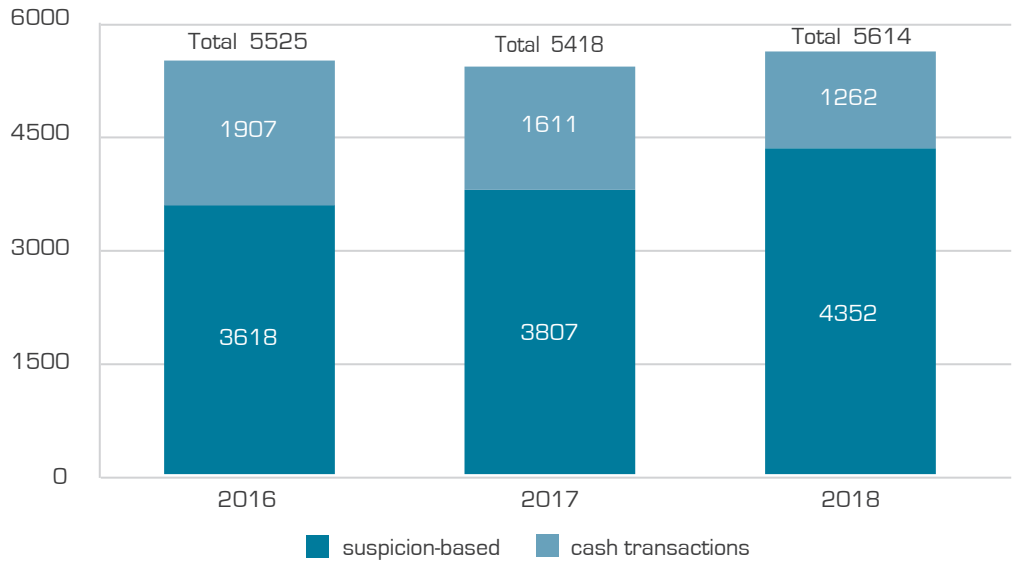


Figure 3. The number of reports received by the FIU between 2016-2018

Note: suspicion-based reports also include reports where the basis of reporting is unspecified.

it stood at 65%, in 2017 at 70% and in 2018 at 77%. Reports on suspected money laundering dominated among suspicion-based reports (95% of suspicion-based reports), while the number of reports on suspected terrorist financing and suspected subjects of the International Sanctions Act was marginal (4% and less than 0.5%).

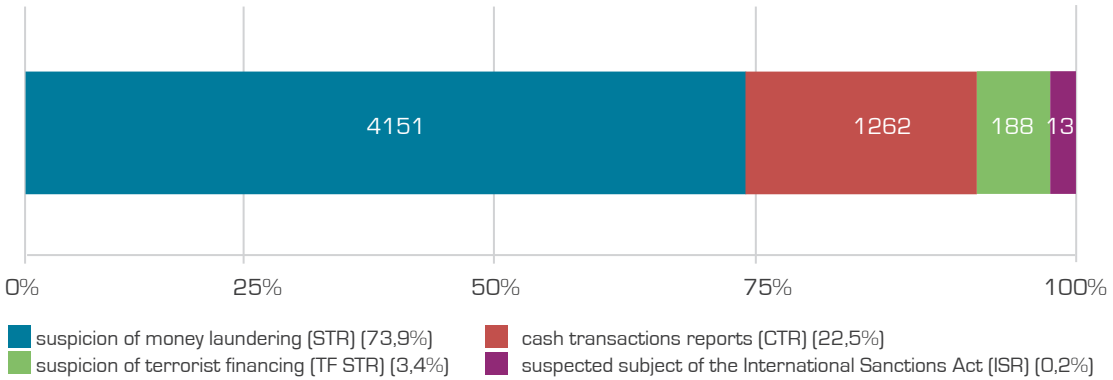


Figure 4. Distribution of reports based on suspicion and sum in 2018

As in previous years, the majority of the reports sent to the FIU in 2018 came from financial institutions and credit institutions (Table 1). Over the past three years, the number and share of the reports sent by credit institutions and foreign authorities have increased, while the number and share of reports sent by financial institutions have decreased.

Table 1. Distribution of reports received by the FIU based on senders between 2016-2018

	2016		2017		2018	
	No. of reports	Percentage of senders	No. of reports	Percentage of senders	No. of reports	Percentage of senders
Financial institutions	2314	41,9	1866	34,4	1407	25,1
Credit institutions	2071	37,5	2313	42,7	2208	39,3
Other private operators	382	6,9	386	7,1	363	6,5
Non-profit associations and foundations			2			
Professionals	182	3,3	206	3,8	228	4,1
State authorities	172	3,1	271	5,0	263	4,7
Foreign authorities	397	7,2	368	6,8	1080	19,2
Other	7	0,1	6	0,1	65	1,2
Total	**5525**	**100**	**5418**	**100**	**5614**	**100**

In 2018, as in previous years, reports on suspected money laundering were sent predominantly by credit institutions and financial institutions (Table 2), but due to the obligation imposed under the Fourth Anti-Money Laundering Directive to forward a report concerning another member state to that member state, the number of reports on suspected money laundering received from foreign states increased significantly. In 2015, the number of reports the FIU received from foreign states stood at 319, in 2016 at 397, in 2017 at 368 and in 2018 at 1,080, which is more than three times the number of reports in 2015. Most of the reports on suspected terrorist financing were sent by financial institutions in relation to transactions made with countries with high risk of terrorist financing or persons originating from such countries. The majority of cash transaction reports were also sent by financial institutions. There have been no significant changes in these trends in recent years.

Table 2. Distribution of reports received in 2018 based on the reason for sending and the sender

	Suspected money laundering	Suspected terrorist financing	Suspected subject of the International Sanctions Act	Cash transactions	Total
Credit institutions	2141	4	6	57	2208
Financial institutions	536	124	4	743	1407
Organisers of gambling	6	52		221	279
Traders	3			69	72
Other private operators	8			4	12
Professionals					
... Auditors	4		1	25	30
... Accounting service providers	6			5	11
... Notaries	51	4	1	111	167
... Attorneys	9			1	10
... Bailiffs	2				2
... Trustees in bankruptcy	1				1
... Providers of other legal service	5			2	7
State authorities	237	2	1	23	263
Foreign authorities	1078	2			1080
Other	64			1	65
Total	**4151**	**188**	**13**	**1262**	**5614**

Similar to 2017, the most common reason for reporting suspected money laundering in 2018 was the termination of a customer relationship due to suspicion of money laundering or failure to submit documents or relevant information necessary for compliance with due diligence measures (Figure 5). This illustrates the banks' efforts to put their customer base in order and to apply enhanced due diligence measures regarding high-risk customers. The number of

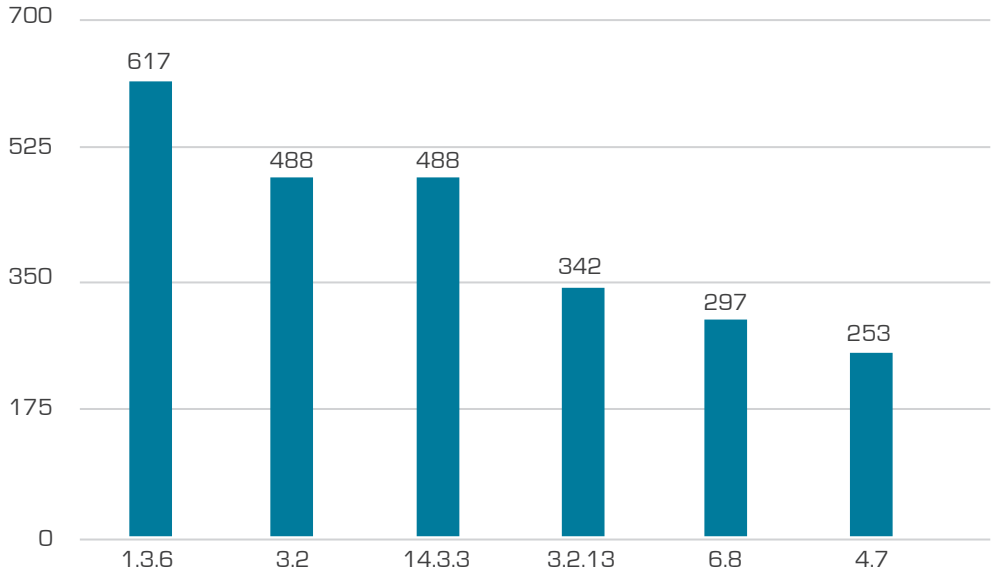


Figure 5. The main reasons for reporting suspected money laundering in 2018

Note:

1.3.6 a credit or financial institution terminates a customer relationship due to suspicion of money laundering or failure to submit documents or relevant information necessary for compliance with due diligence measures

3.2 an unusual transaction on a person's account

14.3.3 a person has an account in the country of destination (reports received from foreign authorities via cross-border dissemination)

3.2.13 other features not listed in the guidelines concerning an unusual transaction on the account, which may indicate illegal activity

6.8 a person makes transactions to other persons in different countries, which does not conform to the customer's usual activities

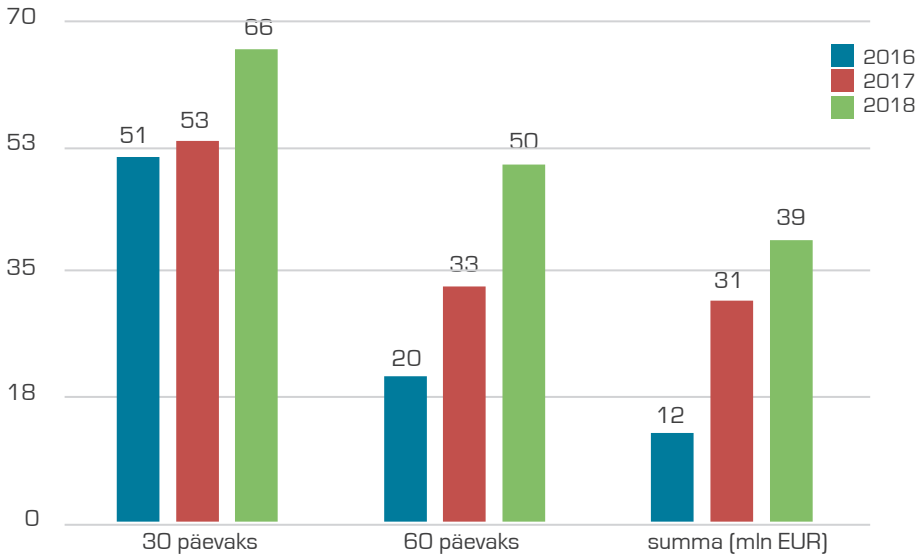
4.7 other features of the customer's activities, which indicate possible money laundering, other offences related to assets or preparation of these offences

reports stating that a person's account was used to make unusual transactions doubled compared to 2017. Due to the significant increase in the number of reports received from foreign states, a new indicator climbed to the top of reporting ranking: "The person has an account in the country of destination."

In the case of transactions suspected of terrorist financing, the most frequent reasons for reporting in 2018, as in previous years, were transfers to countries with a high risk of terrorist financing or transactions with persons related to such countries without opening an account.

3.1.1. Restrictions on the disposal of property

The Financial Intelligence Unit may suspend a transaction or restrict the disposal of property in case of suspected money laundering or terrorist financing. In 2018, the FIU restricted the use of a person's account for 30 days on 66 occasions and for 60 days on 50 occasions (Figure 6). The total volume of assets subject to the restrictions imposed by the FIU was 39.2 million euros. On 23 occasions, property with a total worth of more than 2.3 million was retained by



Joonis 6. Rahapesu andmebüroo seatud pangakontode käsutamise piirangud 2016.–2018. aastal

a court order in criminal proceedings.

In addition, the FIU restricted the use of cash on two occasions for a total amount of 150,000 euros and the use of more than 1,500 prepaid cards.

3.2. OVERVIEW OF THE MATERIALS FORWARDED BY THE FIU

If the FIU decides on the basis of its analysis that an incident may involve money laundering, terrorist financing or related crimes, it forwards its materials to other law enforcement agencies. In 2018, the Financial Intelligence Unit sent materials to other law enforcement agencies on 351 occasions, of which more than a half (around 70%) were responses to queries and materials sent for informational purposes (Table 3). On 52 occasions materials were sent to make a decision whether to commence criminal proceedings, which is significantly more than last year. The remarkable increase in the number of reports of criminal offence was due to a wave of email frauds, in case of which sums paid against false invoices in foreign states were transferred to accounts in Estonian banks. As of 31 December 2018, investigative bodies commenced proceedings in 36 cases (26 cases of money laundering and 9 cases of other offences). On 13 occasions materials forwarded by the FIU were annexed to an ongoing criminal matter, on three occasions investigative bodies refused to commence criminal proceedings and on one occasion the proceedings were commenced in a foreign state. Among the presumed predicate offence for criminal proceedings commenced based on the characteristics of money laundering, there were 14 cases of fraud, eight cases of computer-related fraud, and one case of tax fraud, appropriation, theft and corruption. The number of materials sent to be annexed to an ongoing criminal matter was 95.

In 2018, 101 criminal proceedings on grounds of money laundering were commenced in Estonia. A fifth of them – 26 – were commenced on the basis of the material sent by the FIU (Figure 7).

Table 3. Materials forwarded to law enforcement bodies by the FIU between 2016-2018

	2016	2017	2018
Materials forwarded for investigation	181	242	351
To make a decision whether to commence criminal proceedings	12	14	52
... Criminal proceedings commenced as of 31 Dec	10	13	36
... incl. money laundering proceedings commenced	4	8	26
To be annexed to an ongoing criminal matter	51	59	95
Responses to queries, sent queries, for information	118	169	204
Amounts relating to forwarded materials (EUR)	219,8 million	270,4 million	1,78 billion

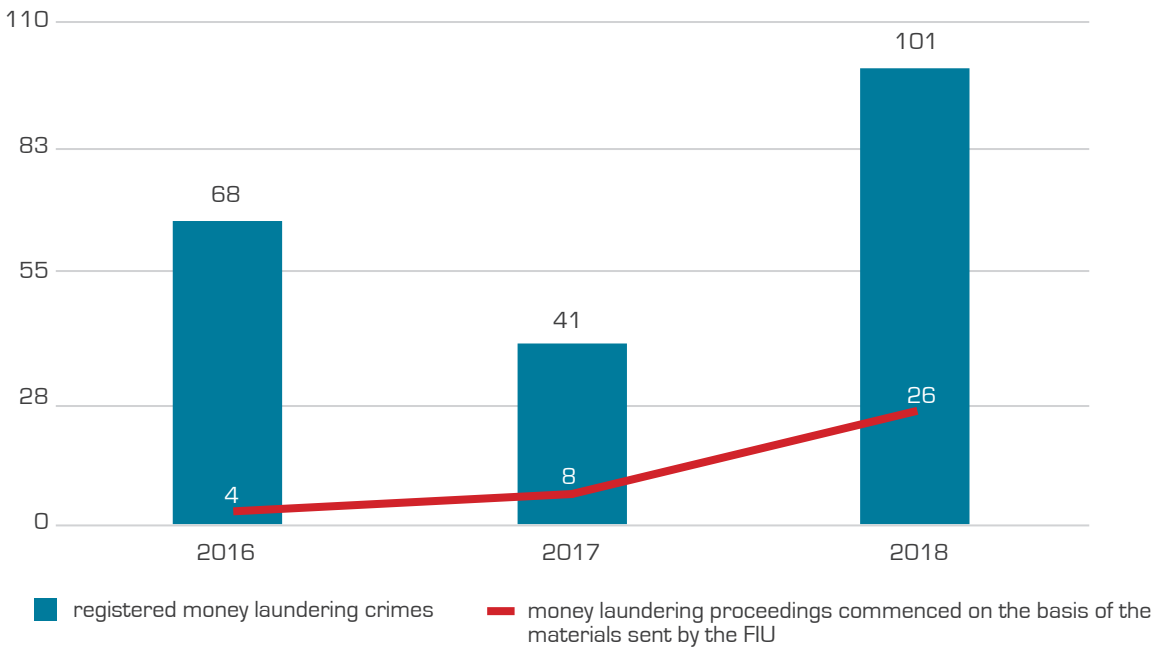


Figure 7. The number of money laundering offences registered in Estonia and the number of money laundering proceedings commenced on the basis of the materials forwarded to the investigative bodies by the FIU between 2016-2018

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

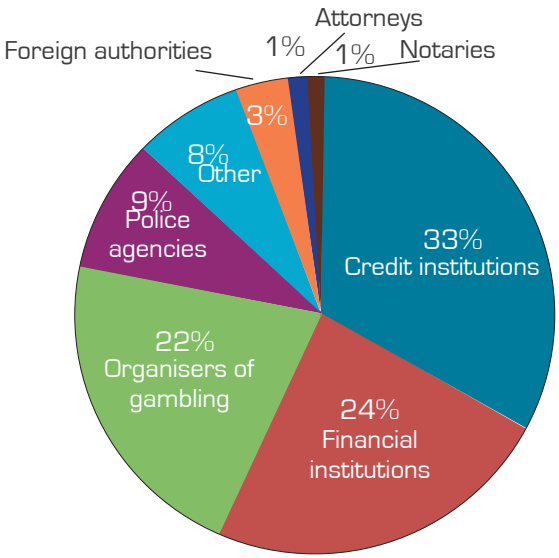


Figure 8. Distribution of reports received by the FIU used in forwarded materials based on the groups of senders

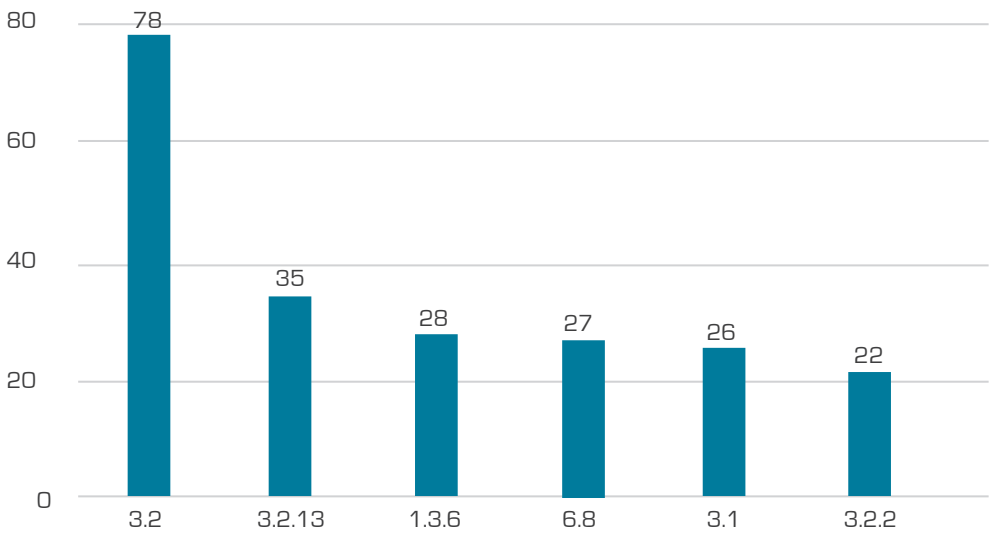


Figure 9. The most common reporting indicators for reports of suspected money laundering used as a basis for forwarded materials in 2018

Note:
3.2 an unusual transaction on a person's account
3.2.13 other features not listed in the guidelines concerning an unusual transaction on the account, which may indicate illegal activity
1.3.6 a credit or financial institution terminates a customer relationship due to suspicion of money laundering or failure to submit documents or relevant information necessary for compliance with due diligence measures
6.8 a person makes transactions to other persons in different countries, which does not conform to the customer's usual activities
3.1 an unusual transaction with cash
3.2.2 a single unusually large cross-border payment that does not conform to normal turnover and/or is insufficiently justified

According to law, the FIU neither forwards the reports received to investigative bodies nor discloses the identity of the sender. However, the FIU keeps records of the reports that serve as the basis for the materials forwarded. Similarly to the two past years, the majority of the forwarded materials were based on information received from financial institutions and credit institutions.

While in 2017 slightly less than 2/3 of the materials forwarded were based on information arising from the cash transaction reporting obligation and in a third of the cases, reports on suspected money laundering were used in forwarded materials, then in 2018 the number of cash transaction reports and reports on suspected money laundering was equal. In both years, a couple of reports on suspected terrorist financing were used in the forwarded materials.

Similarly to previous years, the predominant indicator based on suspicion of money laundering in the reports that served as the basis for forwarded materials was making transactions that do not conform to the customer's usual activities (Figure 9).

3.3. NATIONAL AND INTERNATIONAL COOPERATION

Similarly to previous years, the FIU officials provided methodological support and organised various training activities for obliged entities and market participants in 2018. Overall, in 2018 the FIU officials organised 16 anti-money laundering training activities with approximately 840 participants (Table 4). Employees and professionals of companies falling under different categories of obliged entities and colleagues from the Tax and Customs Board, the Ministry of Finance and the Police and Border Guard Board received training. In addition, the FIU officials took part in various conferences and gave presentations at seminars, workshops, training activities and other events.

Table 4. Training activities organised by the FIU between 2016-2018

	2016	2017	2018
Number of training activities	13	14	16
Number of participants	316	588	841

The FIU's partners include obliged entities, law enforcement agencies and supervisory authorities. The Estonian Banking Association is our good partner that helps to organise cooperation with banks. Both current issues and new trends are under discussion at the regular meetings of the Banking Association anti-money laundering task force. The exchange of information and cooperation with major notifiers and the umbrella organisations and associations of several other obliged entities is also important. The Money Laundering and Terrorist Financing Prevention Act that entered into force at the end of 2017 brought about a number of new situations and issues that required explanation. The exchange of information and responding to enquiries from the obliged entities formed a significant part in our last year's activities.

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

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

In the past few years, significant developments have taken place in multilateral cooperation between the FIU, the investigative bodies, the Prosecutor's Office and the Financial Supervision Authority. Bilateral relations between the FIU and its partners used to dominate the scene, but as the anti-money laundering and related proceedings have gained importance, the level of multilateral and coordinated cooperation between the FIU, the Financial Supervision Authority, the Prosecutor's Office and the investigative bodies is growing. Initiating the establishment of a Financial Crime Group at the Economic Crime Bureau was a substantial step forward in the prevention of money laundering in 2018.

The FIU's cooperation with investigative bodies continues to be close and we continue to cover the resulting solutions for criminal proceedings in our yearbook. For the most part, the FIU is able to gather financial information from foreign financial intelligence units and therefore provides faster identification of movements of money in foreign countries and those committing crimes. Tax fraudsters use many companies and bank accounts set up in foreign countries to cover their tracks. In this field, rapid exchange of information makes it possible to establish subsequent movements of funds and connections between criminals more effectively. We provide information on the prevention, identification and pre-trial investigation of crimes to investigative bodies. An overview of the crime reports, responded queries and other information sent to investigative bodies can be found in Table 3.

Money laundering is often a cross-border offence where the illegal proceeds of a crime committed in one country are transferred quickly through a chain of intermediaries in various other countries to conceal the trail. Therefore, international cooperation is crucial for the FIU. The FIU regularly takes part in the international meetings of the Egmont Group, in the Council of Europe's expert committee MONEYVAL (Committee of Experts on the Evaluation of Anti Money laundering Measures) and the EU's FIU Platform (European Union Financial Intelligence Units Platform).

In 2018, the FIU received 324 queries from more than 47 countries. During the same period, the FIU sent 141 queries to 40 foreign countries (Figure 10). The large number of queries received illustrates the cross-border nature of money laundering offences and the fact that the FIU is contributing to the prevention of money laundering and terrorist financing not only locally but also on an international scale. The average time for responding to foreign queries in 2018 was 18 days.

As before, the closest cooperation in 2018 took place with neighbouring countries. Most foreign queries were received from Latvia (55), Russia (31), Lithuania (31) and Finland (30); and we still received queries from Belarus (16), Ukraine (15) and Moldova (11) quite often. Compared to previous years, the number of queries from Germany, the Czech Republic and Malta and the number of spontaneous exchanges of information increased significantly. Estonia sent most of its foreign queries to Latvia (18), Lithuania (12), Germany, Great Britain and the Czech Republic (10 to all).

With our foreign colleagues, we exchange information on current urgent cases, where in addition to rapid sharing of information, partner institutions can be assisted in imposing temporary restrictions on the disposal of property, as well as part of a more thorough financial investigation alongside criminal proceedings. Operational cooperation between EU Member States takes place in FIU.net, where cases under analysis are still in the phase of seeking confirmation for the suspicion of money laundering. Queries from partner institutions and spontaneous communication point to the growing trend of preferring payment service providers to traditional bank accounts for transferring money. Estonia is being asked for information on cryptocurrency intermediaries more and more often. In addition, we exchange data with other law enforcement agencies via Europol's SIENA system. For instance, in recent years we have often helped to trace the criminal proceeds of drug crime.

Numerous queries from Latvia were mainly related to criminal investigations into tax matters, but the data gathered and analysed in this context suggests that the large-scale cross-border movement of both proceeds of tax crimes and other criminal money may be guided by international organised crime groups. The Latvian National money laundering/terrorism financing risk assessment report for 2018 also mentions the activities of transnational criminal organ-

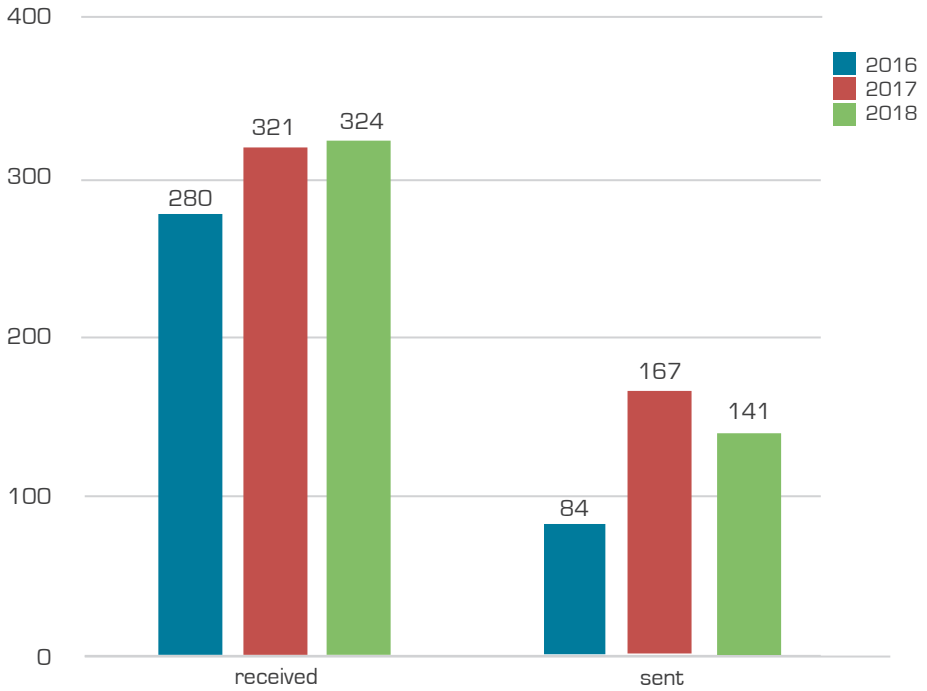


Figure 10. The number of foreign queries received and sent by the FIU between 2016-2018

isations specialising in money laundering in Latvia, Estonia, Russia, Ukraine, Lithuania and Poland.

A number of queries from Russia and Moldova and most from Belarus and Ukraine are sent in as part of the investigations of offences committed in the first half of this decade (mainly tax crimes, appropriations from state-owned enterprises, other corruption, organised money laundering). Many of these cases clearly fit into some recent large-scale money laundering schemes, where money suspected of criminal origin transited through Estonia in the so-called layering phase, and criminals who had very weak ties with Estonia, hid behind shell companies registered in the UK and low-tax countries.

As a general tendency, the number and volume of non-resident deposits has constantly decreased in Estonian credit institutions. However, we have seen signs that some Estonian financial institutions with bigger risk appetite have received some non-resident customers from Latvian banking institutions after the Latvian Financial Sector Development Council obligated their banks to cease business with shell companies in the spring of 2018 due to major international money laundering scandals.

In our previous yearbooks we have already referred to the risk that foreign criminals can take advantage of the opportunity of setting up companies quickly and easily in Estonia. The cases we have analysed show that Estonian companies controlled by foreign individuals are used in the so-called trade-based money laundering, where such a company helps to move assets of unclear origin with fictitious contracts and uses a thin layer of legitimate trade to disguise its activities. Suspicious money from Estonia is often transferred to the accounts of Chinese and Turkish companies. On the basis of both foreign queries received and other case files, suspicious cash flows from the southeast (Belarus, Ukraine, Moldova)

and Russia in recent years can often be attributed to either trade-based money laundering or tax fraud schemes. In addition to the previous years' "commission trade" in building materials, electronic equipment, textiles and consumer goods, large-scale transactions concerning metal and ore, agricultural products, medical devices and pharmaceuticals by Estonian companies led by foreigners stand out.

In cases where

- money only transits through the Estonia financial system, i.e. the account holder is a non-resident and the persons related to the account are likewise non-residents of Estonia,
- the funds from a potential crime originate from a foreign country,
- the funds leave Estonia after being "circulated" on accounts based in Estonia, and
- are used to purchase assets in yet another foreign country,

it is difficult and often impossible to conduct criminal proceedings in Estonia. In such cases, it is more expedient to engage in international cooperation with partner organisations abroad.

Unfortunately, it does not always turn out to be simple or effective, as in some cases, the country where the predicate offences were committed or the destination state where the ill-gotten gains are invested or consumed lack interest or resources to conduct proceedings. At the same time, there are also positive examples where one or both sides have an interest in detecting the crimes committed, identifying the perpetrators and preventing the criminal gains from being placed into the legal economy. The role of investigative journalism, which has become more active in recent years, should be acknowledged, as it has helped to draw public attention to large-scale economic criminal offences, official misconduct and other crimes.

3.4. SUPERVISION

The FIU has a statutory function of performing state supervision over certain market participants. These functions are imposed on the FIU by the Money Laundering and Terrorist Financing Prevention Act and the International Sanctions Act. In 2018 the FIU conducted 6 on-site inspections and 35 remote inspections (Figure 11). Misdemeanour proceedings were started in one case.

Risks arising from Estonia's reputation as a country with a flexible and open environment, in case of which Estonian companies could be used for offering services in other jurisdictions outside Estonia, were already described in the FIU's yearbook for 2016. One of the objectives of supervision proceedings in 2018 was to respond to alerts issued by other authorities, in particular concerning possible unauthorised activities in another country's jurisdiction. If we open our economic space to foreign entrepreneurs for business, we have to bear in mind the arising issues in supervision, including the risk to country's reputation. We have encountered cases where Estonian companies with authorisations granted by the FIU have been used to create a reputation of a lawful and legal service provider, but in a few instances have resulted in embezzling money, and not even in the Estonian economic space. The movement of services to the Internet is increasingly blurring the clear distinction between the services provided, the jurisdictions where those services are provided, and even between the service providers themselves, as combined versions consisting of different components of the aforementioned services that consumers can easily access via their smartphones have become more prevalent. However, this creates new issues for supervision, as in an increasing number of cases it is necessary to ascertain whether and what service is provided, that can be categorised under the activities of an obliged entities over which the FIU supervises, or whether there is any evidence that this service is provided in Estonia.

More detailed statistics on supervisory activities can be found in Table 5.

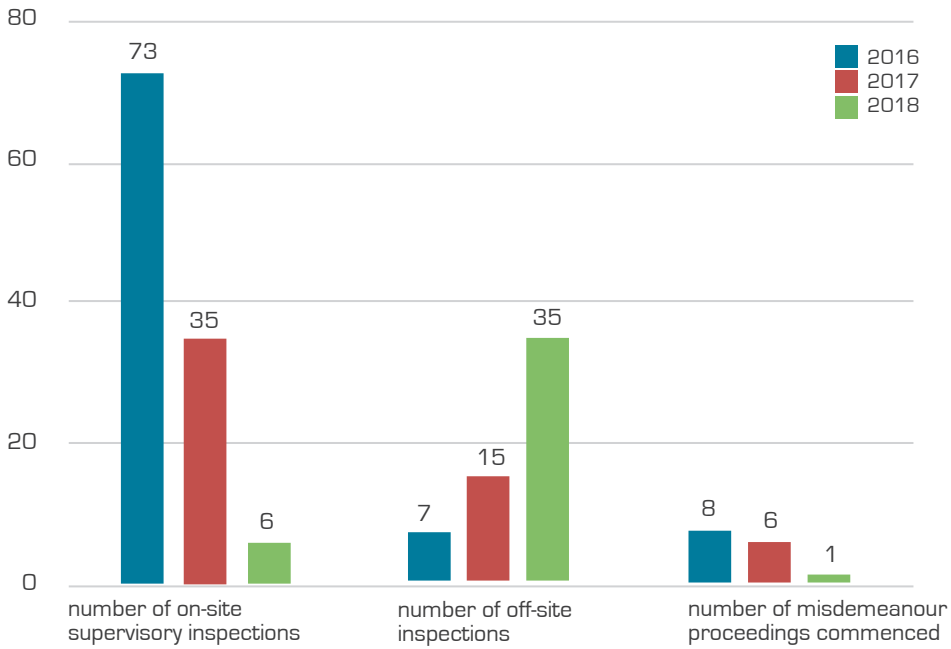


Figure 11. Supervisory inspections and misdemeanour proceedings between 2016-201

Table 5. Distribution of inspections carried out by the FIU in 2018, based on the business activities of the persons inspected

	Total
Providers of a service of exchanging a virtual currency against a fiat currency	26
Financial institutions, providers of foreign exchange services	13
Providers of a wallet service	12
Trust and company service providers	2
Total	41*

Note: * the total is not equal to its parts, as some inspected persons are involved in several business activities.

In the first half of 2018, the FIU focused on inspecting obliged entities operating under a financial institution authorisation, as it received information that foreign supervisory authorities had issued alerts on the activities of several of them. Inspection often revealed that the provision of services in Estonia had not started within six months from issuing the authorisation, so these authorisations had to be archived. There were many situations in which a company authorised by the FIU provided forex trading services on the Internet (not in Estonia) and claimed they had all the required authorisations for such activities, while in reality the authorisations issued by the FIU had not licensed such activities, and some *bona fide* customers encountered problems with recovering their assets or investments. This phenomenon could distort the market to a significant extent, as it indirectly tarnishes the reputation of law-abiding companies, so the FIU decided to focus on these cases. The FIU recommends making sure whose service you want to use, whether the company is in the jurisdiction where the service is to be used, whether the company has the authorisation required to provide the service and whether its background is reliable, before using the service.

In the second half of the year, we focused on providers of

a service of exchanging a virtual currency against a fiat currency and providers of a virtual currency wallet service. In general, similar conclusions could be drawn as in the case of financial institutions – the provision of services in Estonia had not started within six months from issuing the authorisation and another target market had been chosen instead of Estonia.

In terms of supervisory activity, it should be said that the number of applications for authorisations has increased and the resources required for processing them have had a significant impact on the amount of resources invested in supervisory activities.

3.5. GRANTING OF AUTHORISATIONS

The FIU was assigned the task of granting authorisations in 2014. In previous years, the number of applications for authorisations has been much lower than in 2018, when 1430 applications had to be processed. Compared to 2017, the number of applications increased 14 times. Such an increased burden came as a surprise for the FIU and, unfortunately, processing applications used up a considerable amount of resources. It should also be noted that in addition to processing the applications for new authorisations, the FIU is also obliged to revoke, suspend and alter authorisations.

Most of the applications for authorisations are related to

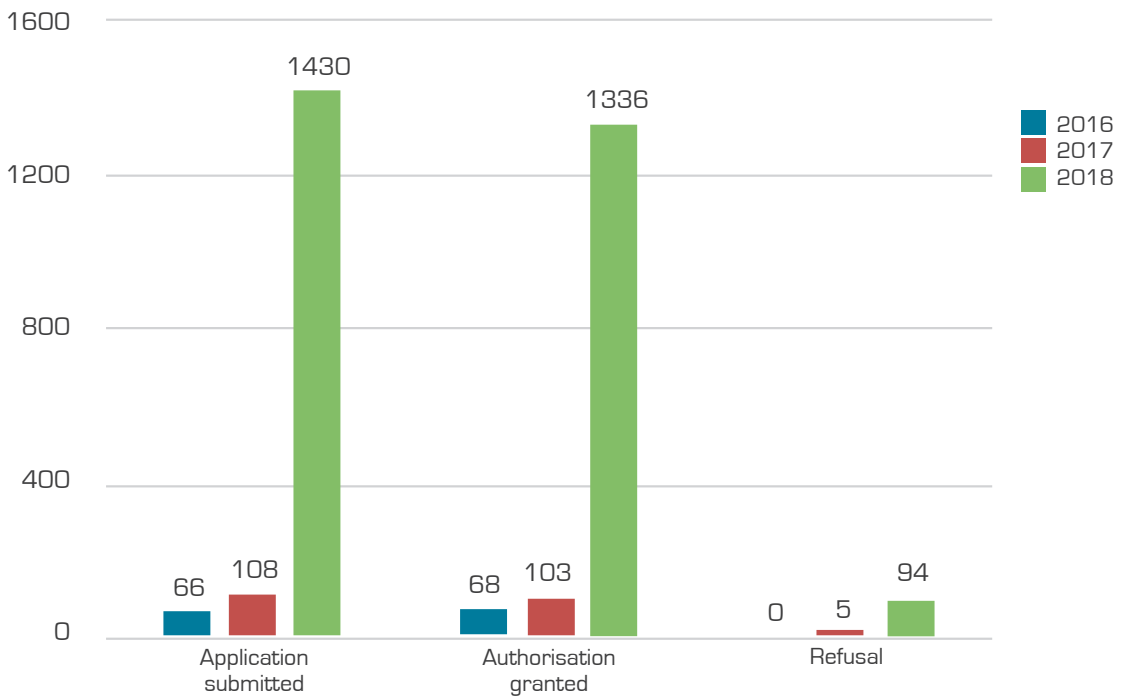


Figure 12. Overview of the applications for authorisations in 2016-2018

the development of technology, i.e. providing a service of exchanging a virtual currency against a fiat currency and keeping it (virtual currency wallet service). These authorisations are mostly applied for together and the applicants are companies whose members of the management body or the actual beneficiaries are foreigners. As a result of this phenomenon, the FIU has drawn attention to the risks involved. The main risks associated with providers of virtual currency include the risk of fraud and embezzlement, the risk of money laundering, the risk of terrorist financing and the risk of applying inadequate due diligence measures laid down by law. The FIU's powers in processing authorisations are not enough to mitigate those risks and the document which certifies the absence of a penalty should not be sufficient for obtaining an authorisation in such a risky field of activity. In order to mitigate the aforementioned risks, we have made proposals to amend legal provisions to set stricter conditions for the authorisation proceedings as well as to amend the regulation applicable to virtual currency providers.

4. COURT DECISIONS ON MONEY LAUNDERING CASES IN 2018

4.1. CRIMINAL PROCEEDINGS

9 court decisions on money laundering entered into force in Estonia in 2018. A total of 16 people, including 14 individuals and 2 legal persons were convicted of money laundering. Most of the money laundering schemes that ended with a court decision in 2018 were similar: people who were convicted used their bank accounts to assist criminals in hiding and laundering their illegal funds obtained from fraud and computer-related fraud committed abroad. We have already described such schemes several times in our previous yearbooks. Below we introduce two money laundering schemes of a different sort that ended with a conviction.

It is worth pointing out the confiscation of assets in court judgments reached in 2018: in case of nine convicted offenders, the judgment also led to the confiscation of their assets, the worth of which ranged from 1742 euros to 163,500 euros. A total of 266,000 euros, along with other assets (including property and a motorcycle), were confiscated from persons convicted of money laundering in 2018. 266 000 eurot, lisaks muud vara (sealhulgas kinnistu, mootorratas).

THEFT OF CEREALS AND MONEY LAUNDERING

Persons whom we refer to by PM, PK, AK and VS were convicted of fraud and money laundering in November 2017. PM was sentenced to 3 years, PK to 2 years, AK to 2.5 years and VS to 2 years in prison on charges of money laundering. Property was confiscated from PM's loved one, a motorcycle and 3250 euros of cash from PM, 57,845 euros from PK and 53,151 euros from AK. The court also satisfied the civil actions of the victims.

From September 2013 to January 2017, the convicted offenders defrauded cereals or oilseed rape worth more than 342,000 euros from the victims. The amounts of fraud varied between 1469 euros and 105,774 euros depending on the victim. The same scheme was used in all of the cases.

PM, PK and AK caused various farmers a misconception that they wanted to buy some cereals. PM or PK acted as a representative of a private limited company X (in case of different victims, the companies acting as buyers also differed) and gave the victim an impression

that the company would pay for the cereals, although, right from the outset, the offenders had no intention whatsoever of doing it. In some cases, PM and PK impersonated another individual (the representative of the "buyer" or company X), i.e. they misled the victim about their identity.

When the sale agreement was concluded, PM quickly arranged for the transport of the cereals. Some of the victims did not receive any payment, while others were paid only the first invoice (about 10% of the agreed purchase price) as an effort to confirm the company's reliability. The remaining invoices were left unpaid.

Either PK, PM, AK or VS arranged for the resale of the purchased cereals to bona fide customers. This was done through the use of various companies, which often belonged to the loved ones of PM, AK or VS (these were not private limited companies, in order to complicate the fraud scheme). The resale price was often lower than what was promised to the victims. After a bona fide customer had paid for the cereals, PK and AK arranged for the transfer of the revenue from the sale to the bank accounts of the various companies to which they had the right of use (in this case, the money was later used for paying different bills) or immediately withdrew it as cash.

THE SALE OF MALWARE AND MONEY LAUNDERING

In September 2018, a person whom we refer to by IZ was convicted of, inter alia, computer-related fraud and money laundering. IZ was sentenced to 3 years in prison on charges of money laundering. A total of 8555 euros of cash and a large number of items worth 20,675 euros were confiscated from IZ. 5 euros and assets with the total value of 4726 euros were confiscated from a third party called TZ and 565 euros and assets worth 11,149 euros from MK. The court decided to substitute IZ's confiscation of assets and entered 65,000 euros into public revenues.

IZ provided third parties with computer programs that can be used for gaining access to computer systems. He generated criminal proceeds with his activity. IZ held and used different accounts in various foreign banks, companies providing digital currency services and companies providing investing services in order to finance his illegal activities and conceal his property deriving from criminal activity, as well as its source, true nature, location and rights of ownership. Different sums from people from various countries were transferred to these accounts. From these accounts IZ made transfers to various platforms and bank accounts under his control, and also withdrew his criminal proceeds as cash. Using ATMs located in Estonia, IZ transferred his withdrawn cash to the bank accounts of his mother TZ and partner MK. In order to conceal his criminal proceeds, IZ used his mother's and partner's bank accounts to make transfers, cash deposits and cash withdrawals, and let them transfer and withdraw cash. In addition, IZ received at least 9586.40 euros in cash and sent 700 euros via Western Union between 26.10.2012 and 31.08.2017.

IZ used his proceeds from criminal activities to finance his illegal activities and pay for daily expenses, commitments and trips. The court established that IZ received at least 344,936 euros, 1,276,765 Czech korunas and 10,575 US dollars in criminal proceeds.

4.2. ADMINISTRATIVE COURT PROCEEDINGS

From the beginning of 2017 until October 2018, no complaints were filed with the administrative court against the activities of the Financial Intelligence Unit.

The only administrative court case was a complaint filed by a company against the FIU's decision not to grant an authorisation as the company did not provide a document which would certify the absence of a penalty for a intentionally committed criminal offence regarding a person related to the company. The proceedings of this dispute are likely to be concluded in 2019.

5. MONEY LAUNDERING SCHEMES

Below, we provide an overview of the schemes analysed by the Financial Intelligence Unit in 2018.

5.1. USING THE DIGITAL WORLD TO OBTAIN MONEY BY DECEPTION

Business email compromise (BEC) scams that started at the end of 2017 also continued in 2018. The success of this fraud was facilitated by the banks' payment systems, which allowed payments to be made even if the beneficiary and the account number do not match. During the year, it became apparent that same players began to recur in different companies whose accounts money was transferred to. Estonian companies that acted as the recipients of money in this fraud scheme operated in different sectors, but none of them was a functioning or high-turnover company. In many cases, the money received on these accounts was transferred further and it is likely that service charges were withdrawn as cash, which indicates that these people were trying to make easy money by allowing criminals to use their accounts. In 2018, we detected more than 5.3 million euros of fraudulently obtained money that had been transferred to the bank accounts opened in Estonia. Funds came from 30 countries. For us, the most exotic of them were Cambodia, South Korea, Mongolia and Bahrain, but it was also sent from most of the European countries, the US, Russia and Turkey. Money that was not withdrawn as cash in Estonia or transferred to the accounts of Estonian companies, moved to various European countries, such as Lithuania, Poland, Finland, the Netherlands and the United Kingdom, but also to the US and some Asian countries.

In addition, during the year the FIU became aware of at least six cases where Estonian entrepreneurs had been affected by such scams and sent money to their foreign partners, however, criminals had previously gained access to their email accounts. And so these entrepreneurs apparently sent money to their partners' accounts mainly opened in Europe, but the account numbers had been changed in emails. We appeal to everyone communicating with foreign business partners to keep in mind that criminals are becoming ever more cunning and looking for new ways of taking advantage of email communication. If your business partner changes their contact details or bank account data, we recommend contacting them by phone or text messages in addition to exchanging emails in order to verify this information.

Sending cash to Africa for romantic reasons or in the hopes of winning money from fictitious gambling games

involve schemes we have already seen. In 2018, the FIU noticed a new kind of fraud scheme in case of which private individuals sent money once again to Africa, more specifically to Benin with the connivance of middlemen. In 2018 we detected 139 money remittances totalling over 75,000 euros. This money was sent to Africa from Tallinn, Tartu, Rakvere and many other places. The incentive to send money has probably come from pages called Touba Financial that have been created on Facebook. These offer loans to private individuals. If individuals contact these kinds of companies, they are charged 119 euros on an arrangement fee. After paying the fee, the customers see the borrowed amount in their account on the company's website, but in order to receive and use it, they have to pay some more. In reality, the person who paid the arrangement fee will not receive a loan. On 05.09.2017 the Financial Supervision Authority issued a warning on its webpage on the activities of Touba Financial, as such a company has no authorisation to grant credit in Estonia.

In our previous yearbooks we have reflected recruitment scams, where "employees" have to send a part of their salary that they have received for work (which was in fact fictitious) to foreign countries. In 2018, a similar wave of fraud sprung up again, but this time people were apparently employed as test clients. A person recruited as part of this fraud explained that while applying for the job, a form at the employer's request had to be filled. The form had to be printed, signed, then scanned and returned to the company. According to the person who had concluded the employment contract, the job was to be a test client, i.e. to monitor how service providers behave and work. So the person claimed to have monitored three companies: one of them provided catering and the other two provided cash transactions. In addition, the person had to check a credit institution's office, where the cash was to be withdrawn. The person explained that the task was to monitor which questions did the bank employees respond to and how did they react. Gathered information had to be sent to the employer as a report. During this fraud scheme, the criminals transferred their criminal proceeds to the bank accounts of the person who had accepted the job. Under the employment contract, the person had to withdraw it as cash and transfer it via a payment institution Western Union. In essence, the employee was knowingly provided with a false impression of what was happening. As a result, the hired employee carried out suspicious transactions in order to conceal the illicit origin of the assets. The Financial Intelligence Unit received information on 10 of such cases, where over 22,000 euros were passed on using the bank accounts of the so-called job-seekers.

5.2. FRAUD TARGETED AGAINST MICROLOAN LENDERS

Criminal groups, who gain their criminal proceeds from deceiving microloan providers, stepped up their activities in the second half of 2018. The FIU became aware of 23 cases totalling nearly 140,000 euros on account of 12 people in 2018. One of them took out loans from eight microloan lenders. The loans varied in amount depending on the microloan provider and ranged from 700 euros to 10,000 euros per transaction. The list of borrowers also contained some people, whose identity documents, which were no longer in the possession of their holders, were used to apply for loans without their knowledge, and so they weren't aware of those cash receipts. The loans were either withdrawn as cash or transferred in which case different borrowers used the accounts of the same private persons. The aim was never repaying them. While Latvian citizens were recruited as borrowers in 2017, in 2018 the accounts of Estonian citizens were used in order to move ill-gotten gains.

5.3. SUSPICIOUS CASH FLOWS IN LEGAL BUSINESSES

One of the aims of money laundering is concealing the real owner or the origin of suspicious cash flows, so that they appear to be legitimate. One way of doing this is to intervene with the operation of a company that is involved in real business and economic activity. If a company has large financial resources, it is possible to add some cash flows masked as invoices or credit agreements without creating suspicion at first. For instance, the company can sell goods that are not actually related to its professional activity, or receive a loan that does not have to be repaid in reality. Those cash flows are shifted through the company and the real origin of the money is concealed from the third party. In order to carry out such a scheme, the companies have to be closely linked through the relationships between their indirect owners or the person shifting the money has to receive hefty fees for using his company as a seller of services in this way. In addition to the usual business activities, the account also shows transit transactions that don't seem conspicuous at first glance and the detection of which requires in-depth analysis. We have identified such schemes in our analyses and it seems that these are rather used for foreign owners and cross-border financing.

Another way is to use this "black money" to gain a competitive advantage for legal businesses, as the received funds do not come from past profits but as leverage that does not need to be repaid.

6. INTERNATIONAL FINANCIAL SANCTIONS

Imposing international financial sanctions did not provide any major surprises in 2018. As expected, the existing sanctions were renewed at EU level and occasionally some individuals were added to or removed from sanctions lists. A major change was brought about by the imposition of restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. Six entities were added to the sanctions list in the middle of the year and nine more at the end of the year.

In 2018, the FIU received 13 reports in relation with suspicion of international financial sanctions but in these cases there was no grounds for the FIU to take action (to freeze assets). It is worth noting that we have taken part in working groups aimed at drawing up additions to the International Sanctions Act in force. It was necessary to update the text of the International Sanctions Act, in particular because the restrictions imposed and the obligation to take measures deriving from European Union law had to be transposed into national law.

7. LOOKING AHEAD TO 2019

The year 2019 will bring a number of important challenges to many participants in the Estonian anti-money laundering system.

A new payment accounts register needs to be launched together with its interfaces with the banks and payment institutions on one side, and the Financial Intelligence Unit and investigative bodies on the other.

A number of financial institutions and other obliged entities need to continue developing their anti-money laundering capacity. Current compliance with the reporting obligation shows that a large proportion of detecting suspicious transactions is targeted at transactions that have already taken place. Real-time screening of suspicious transactions, reporting on them and refusing to carry out transactions are objectives to be pursued by the players of the financial system.

External experts shall assess the quality and weaknesses of the state's anti-money laundering system. In the summer of 2019, Estonia will have to challenge its follow-up report of the fourth evaluation round at a MONEYVAL plenary meeting. We hope to be successfully removed from the follow-up process of this evaluation round and begin to prepare for the forthcoming fifth round evaluation. MONEYVAL's fifth round evaluation will take place in accordance with amended methodology and focus on the efficiency of the system. Adequate risk perception is the first prerequisite for an effective system. Therefore, it is essential that the conduct of the forthcoming money laundering and terrorist financing risk assessment would be thorough and comprehensive. To that end, representatives of state agencies as well as the private sector need to make a contribution. The national risk assessment is the key to understanding all the risks involved, shaping sectoral risk assessments, and mitigating risks in order to plan and perform necessary actions. A risk-based approach to preventing money laundering needs to be put in place and rethought through practice at all levels. Finding the capacity to deal with important matters will inevitably mean giving up activities of low importance.

The AML/CFT Committee and its expert groups have made many proposals for necessary changes in the legislation. Hopefully, policymakers, the government and the Riigikogu will heed the advice of the expert groups and make any necessary amendments to the regulatory environment.

Furthermore, we hope that this year criminal proceedings will give us some news that would bring greater clarity about money laundering to the public and help to clean up our financial system.