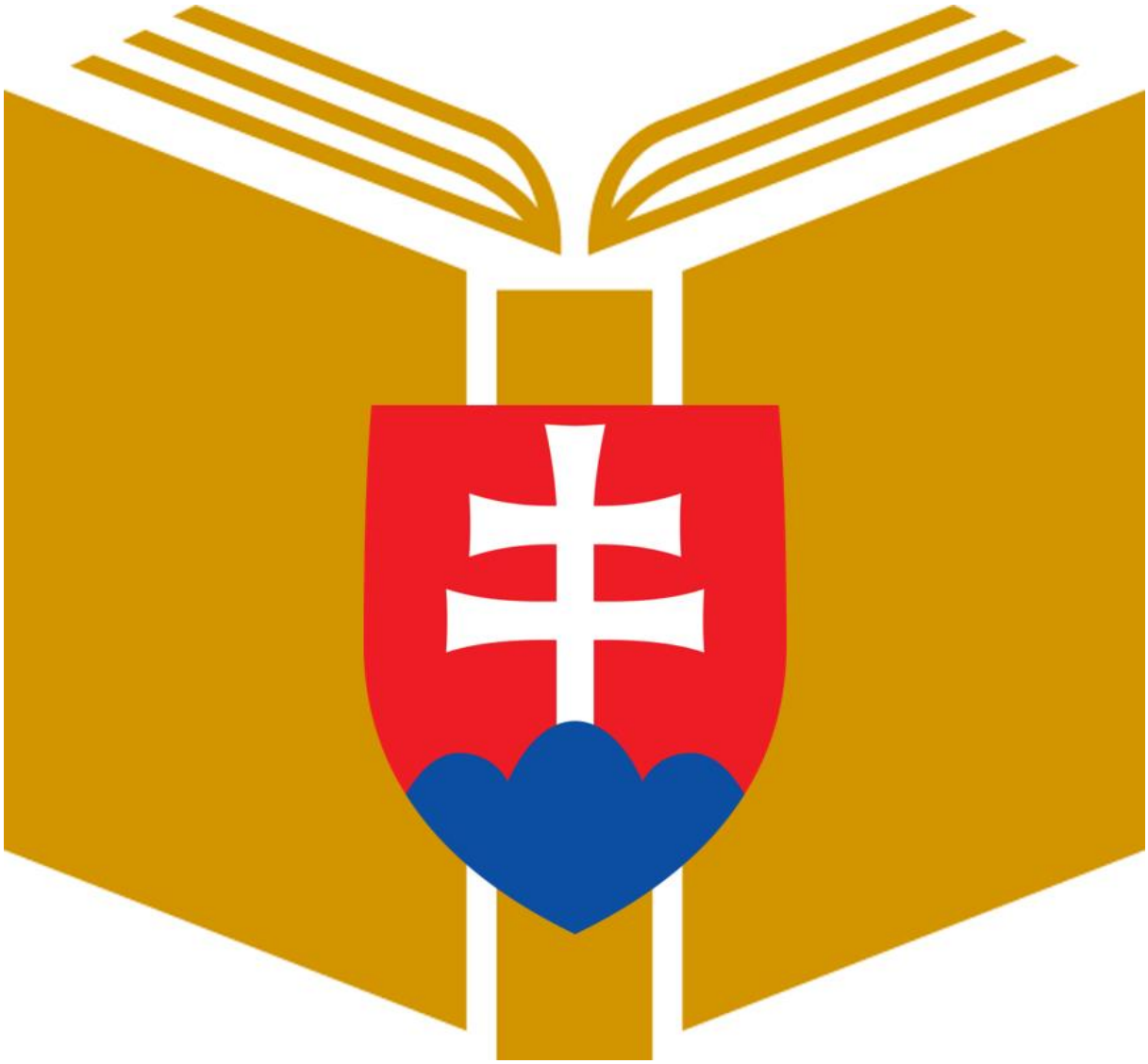
NATIONAL MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT
for 2016-2019



INTRODUCTION

The Slovak Republic is a Central European country and a Member State of the European Union; with its area and population it belongs to smaller countries. The Slovak Republic borders five States: the Czech Republic, Hungary, the Republic of Poland, the Republic of Austria, and Ukraine. The Slovak Republic is not a significant financial centre; it has an open economy and is open to foreign investments which positively affect the economic growth, labour productivity growth, employment growth and the country's competitiveness. At the beginning of the period from 2016 to 2019, the Slovak Republic recorded a positive economic development and unemployment decrease at national level; however, at the end of 2019, the Slovak economy growth decreased which was caused in particular by weak foreign demand. At the same time, the rate and seriousness of crime and other criminal social conduct decreased.

The murder of investigative journalist Ján Kuciak and his fiancée Martina Kušnírová in February 2018 was a turning point considerably affecting the development of the rule of law, democracy and security in the Slovak Republic. The act itself and its investigation caused cross-society public pressure, political and social changes in a broader framework.

In the second round of the National Money Laundering and Terrorist Financing Risk Assessment (hereinafter the "NRA"), the period from 2016 to 2019 was assessed (hereinafter the "assessment period"). In determining the risk level, the content of the related analysis in the Fifth Round Mutual Evaluation Report of the SR in the area of anti-money laundering and counter financing of terrorism measures represented a significant factor as the periods under assessment overlap to a great extent. The Fifth Round Mutual Evaluation Report of the SR was worked out by the Committee of Experts from the Council of Europe Moneyval that assessed the technical compliance of anti-money laundering and counter financing of terrorism measures (legislative framework) and efficiency of these measures. The background data for the Fifth Round Mutual Evaluation of the SR in the area of anti-money laundering and counter financing of terrorism measures was provided by several competent authorities both from the State and private sectors. The evaluating visit of experts from the Moneyval Committee of the Council of Europe took place in Bratislava on 7 – 18 October 2019, and the Evaluation Report was adopted at the 60th Plenary Session of Moneyval (16 September 2020).

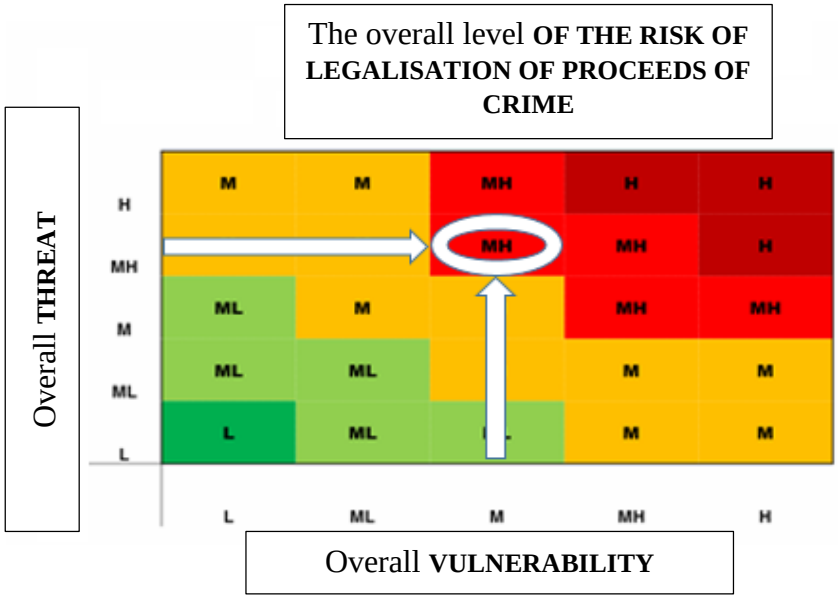
The adoption of the Action Plan to Combat Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction for 2019 to 2022 (hereinafter the "Action Plan") approved by the Government on 7 May 2019 was an important milestone in the area of anti-money laundering and counter financing of terrorism (hereinafter "AML/CFT"). The Action Plan contained measures for the elimination and mitigation of risks identified in the first round of NRA.

In terms of the risk of international legalisation, the Slovak Republic is not perceived as an important country, which is proved by findings and results of the NRA. In the assessment period, several measures were adopted contributing to anti-money laundering and counter financing of terrorism in the legislative area, with several important acts approved, e.g. Act No. 444/2015 Coll. amending 16 acts (the "anti-terrorism package") with effect from 1 January 2016, Act No. 91/2016 Coll. on criminal liability of legal persons and on the amendment to

certain acts, Act No. 315/2016 Coll. on the register of public sector partners and on the amendment to certain acts (act against letter-box companies, which provides greater transparency in business between the State and the private sector), Act No. 52/2018 Coll. amending Act No. 297/2008 Coll. on the protection against the legalisation of proceeds of crime and terrorist financing and on the amendment to certain acts, Act No. 346/2018 Coll. on the register of non-governmental non-profit organisations and on the amendment to certain acts, and, as regards beneficial ownership, beneficial owners of legal persons and pooled asset funds were defined in the AML Act, a central register of beneficial owners was created.

The World Bank's assessment tool adapted to the legal system of the SR was again used in the NRA Project. The NRA Project was coordinated by the Financial Intelligence Unit (hereinafter the "FIU SR"). Eight working teams were created which included 86 representatives of the National AML/CFT Expert Group (hereinafter "NES-LP"). The MJ SR, MF SR, NBS, GPO SR, MD SR, Ministry of Economy of the SR, selected units of the Presidium of the Police Force, SIS, as well as professional associations and chambers appointed their representatives for NES-LP. Five working teams within the NRA Project were focused in risk identification in particular sectors (banking sector, insurance sector, capital market sector, sector of non-financial businesses and professions, sector of other financial institutions), and three working teams were focused on the assessment of threats, vulnerabilities and terrorist financing.

The overall **LEVEL OF THE RISK** of legalisation of proceeds of crime is **MEDIUM-HIGH.**
The overall level of **THREATS** is **MEDIUM-HIGH.**
The overall level of **VULNERABILITY** is **MEDIUM.**



Compared to the previous NRA for the assessment period from 2011 to 2015, the overall level of risk and threat was identified equally as medium-high; a slight improvement was identified for the overall level of vulnerability from medium-high to medium level. The term "legalisation of proceeds of crime" instead of the replaced term "legalisation of income from crime" (money laundering) is used throughout the text of the NRA Report. This change was carried out on the basis of Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts amending Act No. 300/2005 Coll. Criminal Code as amended, changing the name of criminal offence in Article 233 of the

Criminal Code from the original term “legalisation of income from crime” to the term “legalisation of proceeds of crime” with effect from 1 January 2021.

Compared to the first NRA, **a more detailed analysis of the terrorist financing risk** using available FATF methodologies was carried out in accordance with the recommendations from the process of the Fifth Round of Moneyval Mutual Evaluation of the SR. The overall LEVEL of terrorist financing RISK in the conditions of the SR is at **MEDIUM** level. Based on the evaluation of collected information and data, the overall level of terrorist financing THREAT in the conditions of the SR was determined at **MEDIUM** level, and the overall level of VULNERABILITY was determined at **MEDIUM-LOW** level.

The current NRA can be considered transitive not only because it overlaps the process of the 5th round of Moneyval evaluation but in particular with respect to the fact that substantial measures adopted in accordance with the Action Plan following the first NRA started bringing first real results in the area of changed quality of the AML/CFT environment in the second half of 2019, or some of them were adopted only in 2020 with effect from 2021 (e.g., Act No. 312/2020 Coll.). It is also obvious that the related Action Plan should be perceived as a complement to the processes of adoption of measures for the purpose of elimination of the deficiencies found and the recommendations proposed in the Fifth Round Mutual Evaluation Report of Moneyval. The synergy of the above processes is expected to be seen within two years; therefore, the submission of another NRA is assumed in 2024, for the period from 2020 to 2023.

ML THREATS

The module for threat evaluation helps determine a national "level of threat" of money laundering, which is expressed in a five-point scale from "low" to "high". The objective is to draw a conclusion, which areas of the system in the country pose a potentially higher money laundering risk, and which pose a lower risk, in order to be able to respond adequately in these areas and mitigate or even fully eliminate them. Threats are defined as facts or activities of people with the potential to cause harm to the State, society, the economy. The gravity of the threats depends on various general elements reflected in the World Bank's methodology, however, applied to country's specifics. The higher the money laundering threat is, the higher the national level of money laundering threat is.

The assessment of money laundering threats was focused on obtaining data on predicate offences, criminal proceedings concerning predicate offences and the offence of money laundering, cross-border threats, money laundering typologies, trends, high-risk branches, high-risk types of business companies, and the activity of organised crime groups.

KEY FINDINGS OF THREAT ASSESSMENT

THE THREAT OF LEGALISATION OF PROCEEDS OF CRIME IS MEDIUM-HIGH WITH AN UPWARD TREND.

THE SCOPE OF UNRECORDED AND IN CRIMINAL PROSECUTION NOT PUNISHED PROCEEDS OF CRIME IS SUBSTANTIALLY HIGHER.

This key finding de facto has not changed compared to the previous period, partial changes were recorded in framework threats and related trends.

Based on the overall context of long-term criminality development and determination of potential of the type of criminality and individual predicate offences as a source area for the generating of proceeds of crime, an assumed amount of unrecorded proceeds was determined and the following FRAMEWORK ML THREATS AND RELATED TRENDS were set:

		ML threat					Trend		
	Assumed amount of unrecorded proceeds from each offence.	High	Medium-high	Medium	Medium-low	Low	No change	Upward	Downward
Organised crime	the proportion of unrecorded proceeds is substantially higher	X							X
Cybercrime / computer crime in a broader sense	the proportion of unrecorded proceeds is substantially higher		X					X	

Environmental crime	the proportion of unrecorded proceeds is (disproportionally) higher		X					X	
Criminal offences of economic nature	the proportion of unrecorded proceeds is (disproportionally) higher		X				X		
Drug-related crime	the proportion of unrecorded proceeds is substantially higher		X					X	
Corruption crimes	the proportion of unrecorded proceeds is higher		X				X		
Criminal offences against property	the proportion of unrecorded proceeds is slightly higher				X				X
Criminal violence	except for carrying concealed weapons and arms trafficking, where the proportion of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for criminal violence is not significant				X				X
Criminal offences against morality	except for the trafficking in human beings, where the proportion of unrecorded proceeds is higher, the proportion of unrecorded proceeds is not significant for criminal offences against morality				X			X	

Organised crime

The level of ML threat in the cases of organised forms of crime remains high, particularly considering the volume of generated proceeds, volume of unidentified proceeds, nature, societal hazard and scope of related criminal activity for predicate criminal offences with a balanced tendency, however, with the transformation in the area of specific crime, with a substantial shift to criminal offences of economic nature.

As regards the development forecast, it can be expected that criminal activities generating the largest volumes of illegal proceeds will step up; they include tax frauds, in particular VAT frauds, illicit high-tax goods import/smuggling, corruption in selecting suppliers, issuing various permits and allocating subsidies, and the area of drug production and trafficking.

An increase in illicit proceeds for Slovak entities obtaining temporary residence permits for foreigners in the SR, in particular for the purpose of business, will also have to be considered a threat.

The organised form of crime represents a permanent ML threat with unchanged amplitude of trend, however, with a significant change of character of criminal activities towards economic criminal activities.

Cybercrime

In the Slovak context, cybercrime represents an already stabilised, although in terms of forms still dynamically developing, type of crime. The most serious forms of cybercrime represent a medium-high ML threat with an increasing trend but also with an increasing clear-up rate. The proportion of unrecorded proceeds is substantially higher. The recorded attacks in cyberspace outmatch traditional criminal activities and become a horizontal element of it. The existence of digital currencies represents a special threat with the tendency to grow.

In future, it will be possible to observe a high latency of cybercrime in committing criminal offences on social networks in cyberspace. A rise in related black economy can be identified, where the volume, scope and material damage caused by cybercrime will be high with an upward trend.

Environmental crime

In assessing environmental crime, it can be stated that only some forms of environmental crime, in particular illegal activities with waste (illicit import, dumping and disposal), illegal trade in timber and illegal trade in endangered species of wild fauna and flora, have an extensive international dimension; this criminal activity includes high financial proceeds.

Taking into account the unfavourable development in the area of waste management, we expect extensive development of criminal activities in this area, with the expansion of the described practices, such as forgery of documents on waste quantities and types, forgery of documents on legal disposal of waste, and concealing of waste dumping or releasing into the environment with the objective to obtain financial resources by “saving” costs of its legal disposal.

Criminal offences of economic nature

The ML threat of criminal offences of economic nature, in particular with respect to the amount of damage caused and the clear-up rate of criminal offences of economic nature, which ranges from 48.42 % to 52.95 % in the monitored period, is medium with constantly unchanging

tendency of level, where the assumed amount of unrecorded proceeds is (disproportionally) higher.

In terms of ML threat, only some criminal offences have the potential to generate proceeds from criminal offences of economic nature, in particular:

- tax crime, in particular:
a) Tax and insurance premium evasion (**high threat**, downward trend, the proportion of unrecorded proceeds is higher),
b) Failure to pay tax and insurance premium (**medium-high threat**, unchanged trend, the proportion of unrecorded proceeds is higher), and

- certain types of fraudulent acts, in particular:
a) MTIC frauds (**medium-high threat**, upward trend, the proportion of unrecorded proceeds is higher),
b) CEO frauds (**medium-high threat**, unchanged trend, the proportion of unrecorded proceeds is higher),
c) Subsidy fraud and fraudulent bankruptcy (**medium-high threat**, downward trend, the proportion of unrecorded proceeds is substantially higher).

The following represents a special ML threat:

- Distortion of data in financial and commercial records (medium threat, unchanged trend, the proportion of unrecorded proceeds is higher),
- Damaging the European Communities' financial interests and Contrivance in public procurement and public auction (medium threat, upward trend, the proportion of unrecorded proceeds is slightly higher).

ML threat for tax crime is medium-high to high. The expected amount of unrecorded proceeds or the volume of benefit obtained is disproportionately higher than for reported criminal activities. Taking into account the constant transformation of modus operandi of these criminal offences, also despite the adopted measures, the trend of ML threat has not changed except for failure to pay tax and insurance premium with the tendency to increase. There is a significant potential of ML threat in refunding excess value added tax, and criminal activity in the form of carousel fraud (missing trader fraud) is a permanent threat with an upward trend.

Especially, **the ML threat resulting from the abuse of forms and schemes of business companies has to be evaluated as high**, with a significant disproportion between the revealed and latent criminal activity. Without the performance of proactive financial investigation, the volume of generated proceeds identified is substantially lower than the one really generated. **The dynamics of development and transformation of their abuse represents a special challenge for AML/CFT entities.** CEO frauds represent a significant degree of ML threat with a slightly increased tendency in terms of the way of committing criminal activities and the proportion of undetected volume of proceeds generated.

The biggest ML threat can be seen in legal persons operating in the banking sector, sector of commerce and services, brokerage and consulting activities. Limited liability companies and joint-stock companies are the riskiest forms of legal persons used for ML.

In damaging the European Communities' financial interests, there is an ML threat of medium level with an unchanged trend.

Taking into account the assumption that criminal offences of economic nature in the conditions of the SR will have a rising tendency, **the related ML threat will also have progressive character**.

Despite the adopted measures, the potential of generating proceeds through tax criminal activity remains extraordinarily important and represents a high level of ML threat, in particular if this activity is committed in an organised manner, against a background of corruption practices and in a sophisticated way.

Drug-related crime

As regards the generation of proceeds from drug-related and so-called pharmaceutical criminal activity, **we can speak about a medium-high ML threat with an upward trend**, where the assumed amount of unrecorded proceeds is much higher. Its organised form has the same character.

Based on the development it can be expected that **cannabis and methamphetamine consumption,** including their production, import, distribution, as well as an interest in precursors necessary to produce methamphetamine, will further increase.

An **increase in the consumption of new psychoactive substances** connected with their procurement via the internet and abuse of courier and postal services to import them can also be expected. An increase can also be expected in the area of so-called pharmaceutical crime.

These tendencies mean an increase in demand and in consequence, impacts on an increasing volume of proceeds generated by this criminal activity.

Corruption crimes

As regards the threat of generating proceeds of crime, corruption represents a medium-high level of ML threat, without substantial trend fluctuation, in particular with reference to the fact that the assumed amount of unrecorded proceeds is with respect to their character definitely higher compared to the proceeds identified within the really prosecuted corruption criminal activities. However, only large and systematic corruption will continue to represent a real ML threat.

Criminal offences against property

The ML threat of criminal offences against property is medium-low with a downward trend. The proportion of the amount of unrecorded proceeds is slightly higher, however, the fact

that the percentage of overall prosecutions of people in the SR amounts to almost 55.42 percent is an important ML factor. The criminal offence of theft of a high-value thing and organised forms have the biggest potential of generating proceeds from individual criminal offences against property; their assumed amount of unrecorded proceeds is slightly higher. This, however, does not apply to the overall ML threat of criminal offences against property.

Taking into account that a higher rate of latency is expected for the criminal offences against property, the threat of legalisation of proceeds from this type of criminal activity will remain at the same level as so far or it will have a slightly accelerating trend in the segment of high-value things.

Criminal violence

As regards the overall ML threat of criminal violence, we can speak about **a medium-low threat with a downward trend**. However, with the exception of criminal activities concerning **prohibited acquisition and possession of firearms and trafficking in them**, where the proportion of unrecorded proceeds is substantially higher than the value of detected proceeds, the ML threat of this particular criminal activity is **medium-high with an unchanged trend**.

In general, it can be expected that criminal violence will continue to have a marginal significance in relation to possible generation of proceeds of crime and their subsequent legalisation, without a significant change of tendency. The organised form of some types of criminal violence and trafficking in firearms still has to be considered an ML threat.

Criminal offences against morality

In terms of ML threat, **in particular trafficking in human beings** (mainly sexual and labour exploitation, forced begging) **has a potential to generate proceeds of crime**; the proportion of unrecorded proceeds is higher than the value of detected proceeds. Taking into account this fact, the ML threat is medium low and the trend of development remains unchanged. **However, as regards criminal offences against morality as a whole, the share of ML threat in terms of unrecorded proceeds is not significant**.

Within the child pornography criminal offences, the criminal offence of dissemination of child pornography represents a medium-low ML threat with an upward trend, however, in particular in connection with cybercrime. The expected amount of unrecorded proceeds cannot be easily estimated; however, it is definitely higher than for the reported criminality.

In general, **an increase in commercially motivated criminal offences against morality** (pimping, trafficking in women and children, etc.) can be expected; they are a source of illegal proceeds; thus, they will represent the highest rate of ML threat from this type of criminality. The influence and importance of internet for the spread of criminal offences against morality (except pimping cases), which represents a significant factor of ML threat, will further increase.

THE QUALITY OF REALLY INVESTIGATED AND PROSECUTED CASES OF LEGALISATION OF PROCEEDS OF CRIME DID NOT REFLECT THE GRAVITY OF THE DETECTED PREDICATE CRIMINAL ACTIVITY.

COMPARED TO THE 1ST ROUND OF NRA, WHEN CONFISCATION OF PROCEEDS BY DIRECT INSTRUMENTS IN ML CASES WAS IMPOSED TO A MINIMUM EXTENT, THERE HAS BEEN ONLY A SLIGHTLY POSITIVE CHANGE.

POSITIVE TENDENCIES IN THE NUMBER AND VOLUME OF SEIZURES OF PROCEEDS OF CRIME CAN BE STATED. HOWEVER, DESPITE THIS PARTIALLY POSITIVE TREND IN THE AREA OF PROPERTY-RELATED PUNISHMENTS, THIS PROGRESS IS NOT VERY SIGNIFICANT, AND IN THE AREA OF REAL CONFISCATION OF PROCEEDS OF CRIME, IT IS ABSOLUTELY INSUFFICIENT.

THUS, IN GENERAL, THE MECHANISM OF IDENTIFICATION, SEIZURE AND CONFISCATION OF PROCEEDS OF CRIME THROUGH CRIMINAL PROCEEDINGS IS NOT A SIGNIFICANT FACTOR OF RESTRICTION OF "DIRTY MONEY" CIRCULATION IN THE ECONOMY.

The analysis unambiguously confirmed the fact that despite the capability to penalise all types of legalisation (self-laundering, autonomous money laundering or money laundering by third persons), including the penalisation of legalisation of proceeds generated by criminal activities abroad, and even despite an increase in the number of investigations, criminal prosecutions and convictions for legalisation of proceeds of crime, the majority of cases concerned simple property-related criminal offences, and the share of **High Profile Cases** increases only gradually.

In general, despite the adoption of several measures, no stable positive trend in the area of quantitative increase in the number of cases detected, investigated or with conviction in this area can be stated in the period 2016-2019.

Penalising the legal persons for the legalisation of proceeds of crime still remains a challenge.

However, we have registered a qualitative change at the end of 2019 and in 2020; in addition to other factors, it should be imputed to the functioning of measures adopted within the fulfilment of the action plan for the previous NRA (e.g. in the area of financial investigation, in the area of mentality change, adjustment of law enforcement authorities focusing on the application of the follow-the-money principle). In this period, several criminal prosecutions were commenced for the organised form of corruption and other types of criminal offences of economic nature (but for example, also environmental crime) perpetrated in an organised form including the related moment of legalisation of proceeds of crime generated in such a way. In the process of performance of this NRA, however, these criminal cases were mostly within pre-trial proceedings or final decisions of courts still were not available.

Although legal persons are often used as means for legalisation, **no legal person has been finally convicted yet** for ML, however, several investigations are under way.

Despite several convictions concerning organised crime, trafficking in human beings and drugs, the results of penalising the proceeds generated in an organised form of crime are modest.

Absolutely in conflict with the threat identified by the previous NRA – no substantial results were achieved in prosecuting and convicting ML cases in connection with corruption. In this area, too, a positive trend has been recorded since the end of 2019.

The absence of real proactive parallel financial investigation from the earliest stages of illicit conduct and consumption of an act of simple legalisation form to a predicate criminal offence is the biggest source of inefficient system of detection and generation of serious cases of legalisation of proceeds of crime.

In the monitored period from 2016 to 2019, police authorities assessed 336 ML cases, which represents a share of only 0.48 % of the total number of 69,635 of all criminal offences committed.

Despite a certain improvement, statistical data on predicate criminal activities in the phase of commencement of criminal prosecution is still not sufficiently systematically collected.

For the period 2016-2019, the Prosecutor's Office, in connection with legalisation (Articles 233, 234)

- has concluded the criminal prosecution
  - of unknown persons in 421 cases
  - of known persons in 245 cases

out of it, in 149 cases, it brought an indictment and in 17 cases, concluded a plea bargain, and in 10 cases, conditionally discontinued the criminal prosecution

The basic overview of quantitative indicators of criminal prosecution of legalisation of proceeds of crime for the assessed period						
legalisation					TOTAL	trend
	2016	2017	2018	2019	2016 - 2019	
Total number of postponed UTs	199	123	71	65	458	↓
Number of UTs postponed by the obliged entity/FIU	194/5	118/5	69/2	62/3	443/15	↓
Forwarding the postponed UTs to LEAs	148	87	44	43	322	↓
Forwarding FIU information with suspicion of ML to LEAs	388	273	159	145	965	↓

Commenced criminal prosecution	130	209	149	66	554	↕
Concluded criminal prosecution of unknown persons	118	110	93	100	421	↕
Concluded criminal prosecution of known persons of which:	81	75	36	53	245	↕
Indicted people	39	58	20	32	149	↕
Draft Plea Bargain	5	10	0	2	17	↕
Σ	44	68	20	34	166	↕
Interrupted criminal prosecution	105	98	93	8	304	↓
People convicted	17	26	18	13	74	↕
Holding up the proceeds (all obliged entities)	5,565,757	3,062,393	509,659	1,642,993	10,780,802	↕
Seizure of proceeds (only money, €) within pre-trial proceedings – legalisation/ other offences	63/6,078,580/2,416,882	52/3,028,430/17,212,353	52/1,192,072/60,089,430	48/3,449,150/885,144	215/ 13,748,520/ 80,603,810	↑
	252.00%	17.59%	1.98%	389.67 %	17.06%	
Seizure total	8,495,462	20,240,783	61,281,502	4,334,294	94,352,330	↑
Asset-related decisions ML/other – Article 58	4/15	6/23	0/23	1/18	11/79	↑
Article 60	0/821	0/855	1/863	3/560	4/3099	
Article 83	0/51	0/63	0/71	1/17	1/202	
Article 56	1/454	0/496	0/596	1/618	2/2137	↑
Really confiscated proceeds in € based on asset-related decisions in criminal prosecution	71,835.88	76,197.82	1,957,672.11	1,094,999.05	3,201,004.86	↑

The above can be documented by the following findings of the analysis of concluded criminal prosecutions of legalisation of proceeds of crime for the assessed period.

Related predicate criminal offences:

- As many as 58.93 % of acts from commenced criminal prosecutions were committed in the form of fraud. These were in particular frauds committed abroad with the subsequent unauthorised transfer of financial resources, and in this group, an increased rate of frauds based on an instruction given by a "false" manager – CEO frauds – was detected; a share of 12.12 %.
- Thefts pursuant to Article 212 of the Criminal Code (in particular thefts of motor vehicles) follow, with a share of 33.63 %. Other predicate criminal offences[1] occurred only marginally, with a share of 5.95 %.
- **However, this situation did not prove true in assessing finally concluded criminal cases of legalisation of proceeds of crime. Here, criminal cases of legalisation of stolen motor vehicles (almost 19% of finally convicted criminal cases), or associated criminal cases (falsification and fraudulent alteration of motor vehicle identification numbers) continued to dominate. In this type of criminal activity, all types of laundering were identified (self-laundering, autonomous laundering, as well as laundering by a third person). Fraudulent activities and embezzlement represented predicate criminal activity in 9 %. However, here it is important to note that legalisation by a third person or autonomous laundering prevailed. In six cases (4 %), a conviction was achieved, in connection with predicate criminal activity committed in an organised form (autonomous laundering or self-laundering). Counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark was identified as a frequently used instrument for commission of predicate criminal activity or related legalisation.**
- More than one half of proceeds of crime is immediately consumed by the perpetrator of the predicate criminal offence, without special elements of the legalisation moment.
- As regards the services used (products) and sectors and institutions interested, the analysis of all ML cases shows that bank transfers of cash prevail (63.69 % of ML cases) and the other cases include: possession and use (12.80 % of ML cases), ML cases connected with the legalisation of stolen vehicles (originality check, District Traffic Inspectorate and District Office, together with a share of 12.20 %), and conventional sale (6.85 % of ML cases). Other sectors occurred only sporadically.
- Total 491 Slovaks and 368 foreigners participated in ML cases.
- Commission of ML cases and their predicate offences was mostly performed in the territory of the SR, and from the view of possible clear-up rate, the international element only occurs to a limited extent. The analysis of convicted cases shows that **countries, in which the proceeds laundered in the SR were generated, include besides the SR**

[1] Embezzlement, Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors, Breach of regulations governing state technical measures for labelling goods, Forgery and fraudulent alteration of control technical measures for labelling goods, Illicit production of alcohol, tobacco and tobacco products, Human smuggling, Receiving a bribe, Tax and insurance premium evasion, Establishing, masterminding and supporting a criminal group, Damaging the European Communities' financial interests, Subsidy fraud, Credit fraud, Failure to pay tax and insurance premium

(5x) - 2x Czech Republic, 1x USA, 1x Cayman Islands and 1x China. The countries which the proceeds were directed to, placed or legalised in (unless they were place in the – at least eight cases) are as follows: 1 x USA, 1x Poland, 1x China, and 1 x United Kingdom.

- Commission of acts with an international element only appears in cases related to thefts of motor vehicles and frauds (unauthorised transfer of financial resources).
- It is obvious from the above data that **statistically, the laundered proceeds generated in the territory of the SR still prevail**. However, on the basis of quality, a rising trend of detection and subsequent prosecution of money laundering with a cross-border moment of the generation of proceeds of crime has to be stated. This fact is important in particular in the context of an increase in the volume of prosecution of predicate criminal activity, such as carousel frauds. In particular the Czech Republic and Hungary, our neighbouring States, can be considered a relevant regional scope. Ukraine and Austria, as well as Poland follow with a certain gap. No ML cases of legalisation including the involvement of tax havens were produced.
- The assessment in the area of gravity of predicate criminal offences and related volume of seizure of proceeds of crime implies that the most serious offences include: criminal offences in the area of tax, economic and property-related criminality.
- Despite the fact that statistically, nominally only 7.09 %[2] of the volume of legalised property value identified in criminal prosecution was seized, a positive progress has to be stated in the area of seizure of proceeds of crime. For the assessed period, in ML criminal cases, only on bank accounts, the amount of EUR 13,748,519.85 was seized in 89 cases, which means a higher rate of seizure (70% in number and 17% of volume) compared to the executed seizure for all other criminally prosecuted criminal offences (126-times in the amount of EUR 80,603,809.55). Moreover, further volumes of property were covered by other seizure tools (seizure of real estate and movable property other than money on an account). However, this fact was not reflected to a greater extent in the scope of final property-related decisions and in the volume of really confiscated property.
- In connection with final confiscation of proceeds, the analysed court decisions for the period from 2016 to 2019 show that the punishment of property forfeiture was imposed in 11 ML cases[2] (for other criminal offences 79x), the punishment of forfeiture of a thing 4x (other criminal offences 3099x), and a protective measure of confiscation of a thing 1x (other criminal offences 202x). Compared to the 1st round of NRA, when confiscation of proceeds by direct tools in the cases of money laundering was imposed only in minimum cases (e.g., in the previous period, no punishment of forfeiture of a thing was imposed in any ML criminal case), it is a positive development. However, as regards efficiency, it is necessary to also consider the above-mentioned share with

[2] It is data for criminally prosecuted ML cases Article 199 table Module 1B – Total detected value of financial resources EUR 193,817,782.82 in relation to Total value of seized financial resources. However, the data provided does not take into account currencies other than EUR because conversion into EUR is impossible. Other resources in the currencies CZK, USD, PLN, GB were also seized; however, they are not included in the total amount of seized financial resources.

confiscations for other criminal offences, and in particular the issue of real confiscation of proceeds of crime as a consequence of such court decision.

ML VULNERABILITY

The vulnerability of the country assesses the mechanisms of measures used by the SR in combating money laundering.

The overall level of vulnerability of the SR was evaluated on the basis of the country's capacity to combat legalisation and of the overall vulnerability of national economy sectors. **THE OVERALL VULNERABILITY OF THE COUNTRY in terms of fight against legalisation of proceeds of crime was evaluated at MEDIUM LEVEL**. The country's capacity to combat legalisation was evaluated at medium level. The country's capacity to combat legalisation of proceeds of crime represents the country's capacity to prosecute and punish the cases of criminal offence of legalisation and the country's capacity to seize proceeds and means of crime. The overall vulnerability of national economy sectors in terms of fight against legalisation of proceeds of crime was evaluated at medium to medium-high level.

Medium to medium-low vulnerability concerning the quality of investigation, criminal prosecution, judgements and quality of property seizure framework was identified. Out of the sectors under evaluation, the highest vulnerability was evaluated in the banking sector and sector of asset management companies.

Selected vulnerabilities in the system of measures against legalisation identified during the NRA (other vulnerabilities are identified in the assessment of sectors).

1. Beneficial owner:

- low efficiency of implementation of data on beneficial owners into source registers was identified, resulting in the insufficient loading of the Register of Legal Persons, Entrepreneurs and Public Authorities (hereinafter the "Central Register") with data on beneficial owners,
- no efficient mechanisms to verify the correctness and timeliness of data on beneficial owners of legal persons in providing it to respective source registers have been adopted,
- no efficient mechanisms for the application of adequate and dissuasive sanctions in the event of detecting violations in connection with the provision of data on beneficial owners have been adopted,
- the Slovak legislation does not regulate the duty to keep information on beneficial owners of foreign trusts (or similar legal groupings) in the Central Register when a citizen of the SR permanently residing in the SR is the administrator of the foreign trust or if the administrator of the foreign trust is resident outside the European Union and such administrator of the foreign trust establishes a business relationship in the SR or acquires immovable property in the SR on behalf of the foreign trust,
- the legal persons, which provided data on beneficial owners to the register of public sector partners (this register is not a source register for the Central Register), are not obliged to provide information on beneficial owners to the Commercial Register (the

Commercial Register is a source register for the Central Register), which can cause a lack of data on beneficial owners in the Central Register.

As the Slovak legal system permits the operation of silent partners in Slovak legal persons, it is reasonable to pay increased attention to the operation of silent partners in connection with the issue of beneficial owners in Slovak business companies.

2. Bonds:

- the issuance of bonds by legal persons is not restricted, a legal person may issue bonds without limitations in any scope. The Central Securities Depository cannot refuse the registration of an issue, for example, due to doubts about the issuer's financial standing or purpose of the issue. Legal requirements for the registration and issue of bonds need modifying, for example, in the event of unusually high volumes of issues, for foreign issuers (with a link to off-shore countries) etc.

3. Cash payments:

- for money laundering, perpetrators of criminal offences prefer cash as it allows uncontrollable movement of financial resources outside the financial system, as well as their cross-border transfer. The objective of such activity is to prevent the detection of origin of the financial resources obtained from criminal activities. The use of cash payments does not require any special knowledge or planning abilities. Cash payments represent an increased risk en bloc for all sectors. The fines imposed for committing a delinquency or administrative delinquency in connection with the limitation of cash payments pursuant to Act No. 394/2012 Coll. on limitation of cash payments do not have a dissuasive effect.

4. Provision of collaboration to state authorities:

- the action of state authorities against the business entities (in particular the business entities with a virtual registered office), which do not provide collaboration during control, is time-consuming and inefficient. It is necessary to improve the cooperation of state authorities and also to consider an amendment to legislation in several legal regulations:
- a failure to provide collaboration during a control of an obliged person pursuant to the AML Act – the entity does not pay the imposed fine and the proceedings are time-consuming,
- if the entity is a tax debtor and, at the same time, a "letter-box company", which, in general, could not be contacted by the tax administrator already in the past and which could only be solved by imposing a tax and sanctions, if any, in such case outstanding taxes usually increase and it is suitable to carry out operative activities by the police,

and it is necessary to speed up hand-over of information between tax administrators and police within the operational procedures which would allow timely adoption of measures on both sides.

5. It is necessary to carry out fully fledged financial investigation. There are no trainings in financial investigation including virtual currencies, there is no professional education in the area of fight against legalisation, the support of analytical activity focused on the detection of complex schemes of serious economic and corruption criminal activity is insufficient.

6. Insufficient efficiency of mechanisms of detection and seizure of proceeds of crime, (the vulnerabilities should be eliminated by adopting Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts, which came into effect on 1 January 2021, and will provide for efficient tracking, seizure and confiscation of proceeds of crime and introduction of clear and effective rules for seized asset management and disposal; the act on central record-keeping of accounts is in the legislative process, it is expected to come into effect on 1 December 2021).

7. In several cases, it is very difficult to identify the perpetrator of a predicate criminal offence, it is also impossible to finally identify the form of money laundering, i.e., to find out whether the person, who had lured out the financial resources fraudulently, is the same (or another) person as the person, who subsequently handled the resources as the owner of/the person holding the right of disposition over the bank account concerned. The way of commission of some of these acts suggests that several persons are involved acting in a coordinated manner in various States (which is suggested by testimony of witnesses usually implying that the perpetrator of the predicate criminal offence communicated with them in writing in their language, the e-mails did not contain any grammatical error and probably the communication was not translated using the available internet translators), or that the activity was committed through organised groups.

8. Customs authorities should improve their knowledge of ML/FT risks and related duties in this area and develop reliable mechanisms allowing revealing false declarations or no declarations of cash transportation and suspicions of ML or FT,

9. In the sector of non-financial business and professions, it is necessary to increase obliged persons' awareness of measures against money laundering and terrorist financing; in the sector of gambling games, a higher risk is posed by deposits into players' accounts in virtual currencies or through Paysafecard and Skrill (virtual wallet).

10. The absence of a central register of accounts and improvement of efficiency of the act on proving the origin of property.

RISK OF LEGALISATION OF PROCEEDS OF CRIME AT NATIONAL LEVEL

1. THE LEVEL OF THREAT OF LEGALISATION OF PROCEEDS OF CRIME AT NATIONAL LEVEL

Several factors, including the general development of criminality, and the current characteristics and expected trends of criminal activity were analysed for the purpose of identification of the ML threat in the SR.

In determining the threat of unreported crime amount, the working group selected the following evaluation:

- the proportion of unrecorded proceeds is not significant,
- the proportion of unrecorded proceeds is slightly higher,
- the proportion of unrecorded proceeds is higher,
- the proportion of unrecorded proceeds is substantially higher,
- the proportion of unrecorded proceeds cannot be estimated.

The analytical activity was based on

a) regular analytical and assessment reports and documents of decisive actors operating in the area of fight against crime, in particular:
    - Reports on the Security Situation in the SR for the respective calendar years 2016 to 2019,
    - **Reports of the General Prosecutor of the SR on the activity of the Prosecutor's Office and knowledge of the Prosecutor's Office of the state of lawfulness in the SR, and Reports of the Special Prosecutor on the activity of the Special Prosecution Office and knowledge of the Special Prosecution Office of the state of lawfulness for the respective calendar years, and the respective statistical yearbooks of the GPO SR,**
    - **Annual Reports of the Financial Intelligence Unit,**

b) Special assessment and analytical documents, typological studies,
c) Special, ad hoc analytical outputs with the involvement of a wide spectrum of investigators, prosecutors and representatives of the Ministry of Justice[3],
d) Fifth Round Mutual Evaluation Report of the SR in the area of anti-money laundering and counter financing of terrorism measures worked out by the Committee of Experts (Moneyval),

[3] E.g., within the Prosecutor's Office, prosecutors were appointed for each part, who directly systematically participated in the process of threat assessment within the NRA

e) as well as the data and sources of the third sector and evaluations of the SR by international organisations, where these were reflected in relation tothe statistical data produced on the basis of the structure and within the scope of the World Bank's methodology from all actors of the process (police authorities – Criminal Police Office and NAKA (National Crime Agency), OSISP (Department of Administration of Police Information Systems), authorities of the judicial system and Prosecutor's Office, FD SR and Customs Criminal Office, intelligence service and academic community).

The working group focused on the creation of cohesion of quantitative and qualitative indicators with the highest possible informative capability. In particular, it endeavoured to include in the analysis the scope and impacts of unreported criminality, whose rate was mainly affected by the intensity of formal and informal control, tolerance of the injured people, the level of legal conscience, crime type, etc.

Using the experience from the previous NRA, in order to obtain a comprehensive view, the working group also focused on the source crime generating income from criminal activity, which should be subsequently legalised, performed a comprehensive analysis, which was supplemented with the application of the module according to the World Bank's methodology.

Based on the decision of the team and with reference to Article 27 of Act No. 297/2008 Coll., data of the Department of Administration of Police Information Systems of the Presidium of the PF and of the General Prosecutor's Office of the Slovak Republic was considered to be the basic information source. A special part of data consisted of information obtained by "manual" assessment in accordance with the module 1B[4] (see more details in Part 3 of this analysis), which only confirmed the above facts.

Based on this approach within the module for threat assessment, the working group identified:

- sources of threats – the areas of criminality producing the biggest volume of proceeds of crime and related main predicate criminal offences,
- the follow-up trends and procedures used in money laundering – forms of placing and methods of coverage of the origin of resources from criminal activity, and
- identification of the scope of non-penalised legalisation of proceeds of crime.

[4] Data from tables of Module 1B – from the level of police, GPO SR and MJ SR.

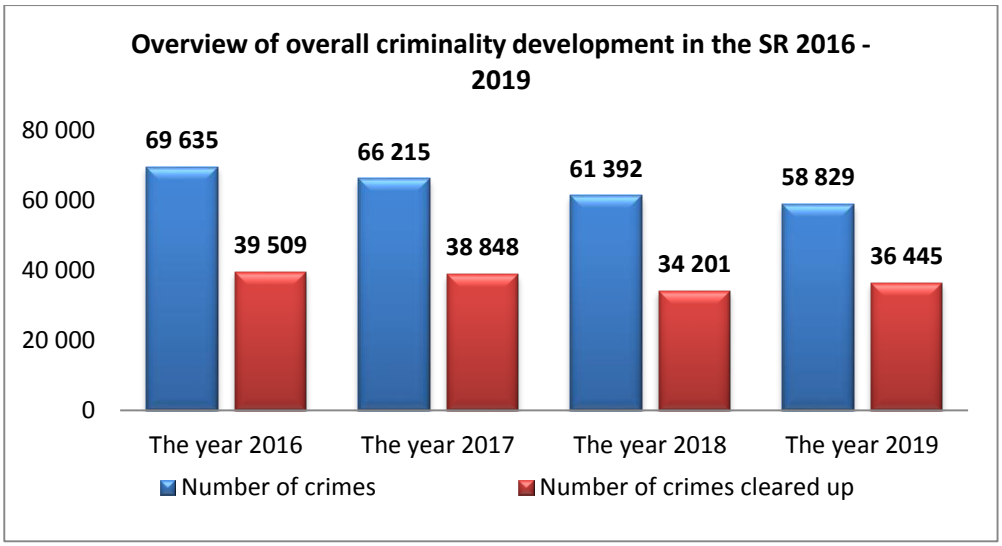
2. ASSESSMENT OF BASIC SOURCE ML THREATS RESULTING FROM INDIVIDUAL TYPES OF CRIMINALITY AND RELATED FORMS OF COMMISSION OF CRIMINAL ACTIVITY

FACTORS OF ML THREATS IN THE CONTEXT OF ANALYSIS OF DEVELOPMENT OF INDIVIDUAL TYPES OF CRIMINALITY IN THE SR

The underlying assumption for the assessment of money laundering threats is to understand the general context of long-term development of criminality in the conditions of the SR and its influence and factors affecting the scope and volume of the generation of proceeds of crime.

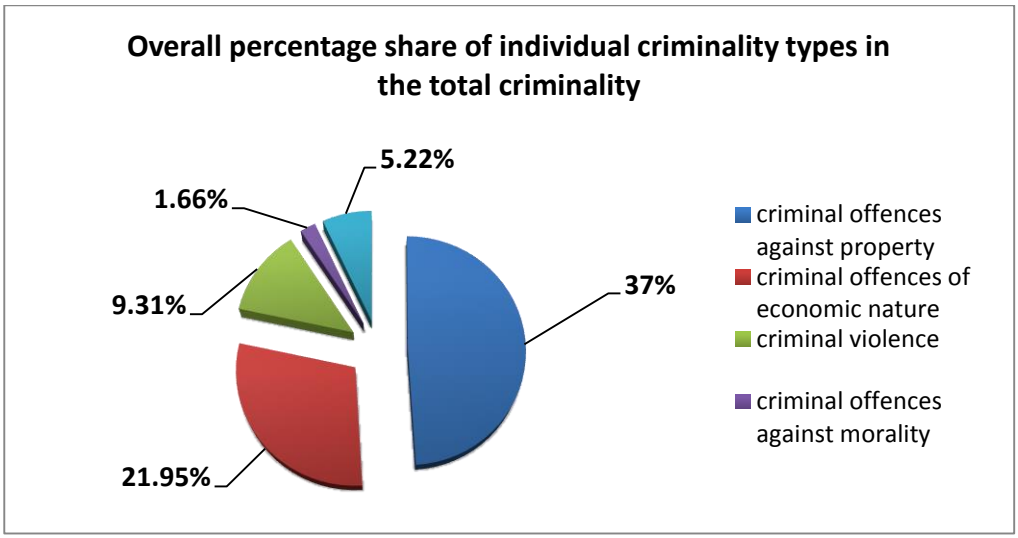
A number of factors affecting the commission of criminal activity need to be considered. However, as regards the ML threat, primarily it is the motive of perpetrators to generate profits (proceeds), i.e., the reason why they commit the criminal offence, and **the determination of the potential of a type of crime as a source area of the generation of proceeds of crime**.

In terms of the number of detected criminal offences, the development of the security situation in the territory of the SR can be considered extraordinarily positive. Both in the first assessment period and in 2016 to 2019, a **significant decrease in detected criminal offences** was recorded; **thus, we can definitely speak about a gradual downward trend** of the total number of reported criminal activity (2016 – 69,635 detected criminal offences; 2019 – 58,829 detected criminal offences).



Criminal offences against property have been dominating in the long term in the structure of criminal activity recorded in the territory of the SR; in the monitored period they represented from 33.29 % to 39.41 % of the total number of detected criminal offences. Criminal offences against property were followed by criminal offences of economic nature ranging from 21.39 % to 22.65 %, and criminal violence from 9.16 % to 9.42 % of total criminality. Frauds and tax criminal offences create a specific group within criminal offences of economic nature, amounting to 15.66 % to 27,62 % of criminal offences of economic nature

for frauds, and from 31.36 % to 42.87 % of criminal offences of economic nature for tax criminal offences.



As regards the identification of ML threats, it is important to distinguish among individual types of criminality; for the needs of the NRA, criminal offences within individual types of crime were identified, which generated the highest damage[5], and they were subsequently taken into account in individual statistical data.

In the monitored period, a downward trend was recorded for criminal offences against property, criminal offences of economic nature, as well as criminal violence. A slight increase in criminal offences against morality was recorded in 2016 to 2019. The development of tax criminal activities is stabilised, and varied progress was recorded for corruption crime.

For the purpose of identification and assessment of ML threats resulting from individual types of crime and related forms of commission of criminal activity, the following were separately analysed:

- Criminal violence (2.1.)
- Criminal offences against morality (2.2.)
- Criminal offences against property (2.3.)
- Criminal offences of economic nature (2.4.) a
- Special partial types of criminal activity:
    - Corruption crimes (2.5.)
    - Drug-related crime (2.6.)
    - Organised crime (2.7.)
    - Cybercrime (2.8.)
    - ML threat from the view of SOCTA (2.9.)
    - ML threat in environmental crime (2.10).

[5] The issue of relation between **damage and proceeds** of crime is discussed below.

2.1. Criminal violence [6]

2.1.1. ML threat factors

In terms of ML threat, only certain types of criminal violence have a potential of generating proceeds of crime.

As regards the formal classification of criminality, this area includes in particular prohibited acquisition and possession of firearms and trafficking in them, for which the proportion of unrecorded proceeds is substantially higher than the value of detected proceeds, ML threat is medium-high and the trend of development is without change.

The overall ML threat of criminal violence is medium-low with a downward trend.

The share of criminal violence in the overall criminality is about 2 % with more or less balanced tendency. Most violent criminal offences for the monitored period were recorded in 2016 – 1514 cases. In the next years, there was a slight decrease in the percentage of the total number of detected criminal offences, and in 2019, there were 1299 cases. As regards development, we can speak about a relatively stabilised development of this criminality in respect of detected cases, clear-up rate, as well as the reached percentage of the total number of detected criminal offences.

When assessing the development compared to the previous state found during the first NRA, it can be stated that there was a **significant decrease in the number of violent criminal offences**, **by 40% -** from 9032 to 5507. The reason behind the decrease was the intensified work of the police in the area of prevention, an increase in the number of patrols in preventing street criminality - robberies, better security measures applied to structures (banks, gambling venues, etc.), prevention of crimes against elderly people, etc.

For the monitored period 2016 to 2019, there were 2409 cases of conviction for criminal violence (43.74 % of the total number of violent criminal offences), and in 10 cases, the penalty of forfeiture of a thing was imposed, in five cases the penalty of forfeiture of property, and in 18 cases, the protective measure of confiscation of a thing.

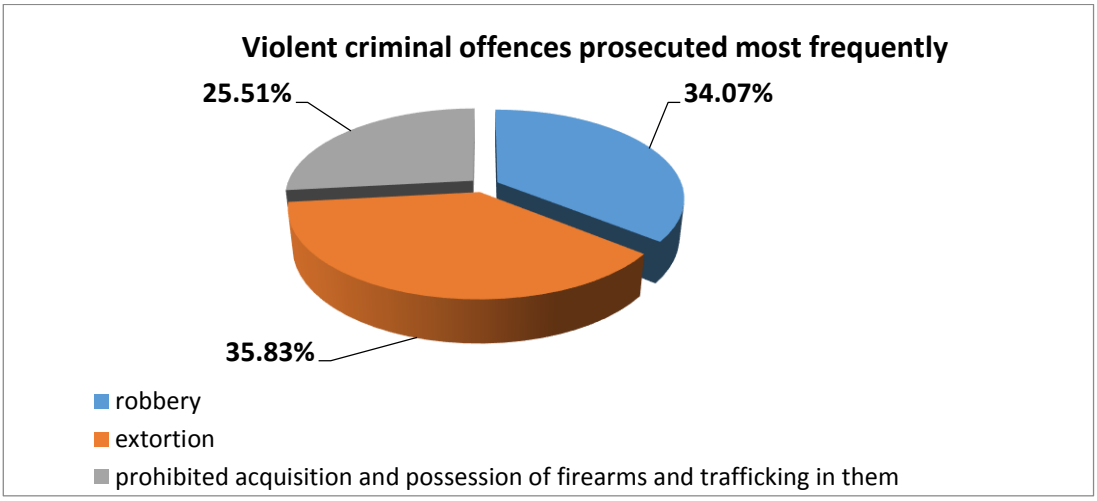
Damage caused by criminal violence amounts to EUR 20,691,000.00, **which is a share of 0.75 % in the overall damage**.

Perpetrators of criminal violence used firearms to strengthen the threat and often committed their act in a particularly brutal manner. Mostly, they were under the influence of alcohol, and cases of commission under the influence of drugs were also recorded. The perpetrators were predominantly young and middle-aged people, who utilised their physical predominance over victims, such as women, children or elderly people. The motive of conduct

[6] Premeditated murder Article 144, Murder Article 145 (old Article 219), Robbery Article 188 (old Article 234), Extortion Article 189 (old Article 235), Gross coercion Articles 190, 191 (old Articles 235a, 235b), Prohibited acquisition and possession of firearms and trafficking in them Articles 294, 295 (old Articles 184a, 185)

for this criminal activity was a poor financial situation; the perpetrators concealed their identity by masking. The perpetrators were interested in particular in financial resources, mobile phones, jewellery or other personal belongings and documents. The profit/proceeds of crime are the subject of the perpetrator's private consumption.

The composition of the most serious and most frequently prosecuted criminal offences has not changed compared to the previous assessment, it includes robbery, extortion and prohibited acquisition and possession of firearms and trafficking in them. **There was a change in relation to ML area, where extortion remains and robbery is a new criminal offence (previously serious threats).**



There is a gradual decrease (1st round of NRA - 2479 cases, 2nd round of NRA – 1973 cases) for the criminal **offence of extortion, which carries along potential legalisation continuation**. Most frequently, the criminal offence of extortion was committed by juveniles and unemployed people, who used weapons, and cases committed under the influence of alcohol or drugs were also recorded.

In this context, it is necessary to perceive a medium-low degree of ML threat only in the cases of serious criminal activity of extortion prosecuted within the competence of the SPO. In particular members of criminal groups are included because extortion is among the ways in which they obtain illicit profits. However, the trend of ML threat is considerably decreasing.

As in the previous assessment, street robberies represent the biggest percentage of **criminal offences of robbery**.[7] In this criminal activity, equally as in the previous period, victims were in particular randomly selected individuals; the perpetrator or perpetrators used the situation, attacked the person without preparation and under the threat of violence, using violence or a weapon, they robbed them (in particular cash, mobile phones). During robberies in structures (shops, betting offices, gambling venues, casinos, banks), the perpetrators escape in general along an escape route prepared in advance, and to commit this criminal activity, they use settled and busy areas to be able to merge into the crowd and escape a possible pursuit and

[7] In terms of long-term statistical reporting and with respect to the character of the criminal offence, the criminal offence of robbery is included in criminal violence.

detection.

Compared to the previous period, the overall damage caused by the criminal offence of robbery recorded a significant decrease from EUR 8,902,000.00 to EUR 2,572,000.00, which represents a share of 0.09 % in the overall damage. The motive of activity in robberies was a poor financial situation, which the perpetrators tried to solve by robbing people, who were expected to give in easily (elderly people, women), and through robberies in structures, where sufficient amount of financial resources was expected. **The level of ML threat for robbery is medium-low with a downward trend.**

For individual years of the assessed period 2016-2019, it can be stated that the occurrence of **premeditated murders** was comparable in individual years, ranging from 16 cases in 2019 to 22 cases in 2018 (2016 – 17 cases, 2017 – 20 cases). Compared to the previous assessment period, there was a slight increase in premeditated murders.

Premeditated murder is a criminal offence very similar to the criminal offence of murder. The difference is in its objective aspect, i.e., in the perpetrator's motive considered in advance to kill another man, and is characterised by planning with the use of a moment of correct timing of the execution. We can say that these are murders to order and for money. It still applies to this most serious criminal offence that its investigation poses particular challenges to the way of documenting, including related financial aspects.

In connection with the commission of the criminal offence of premeditated murder in the assessed period, no investigation into the criminal offence of legalisation of proceeds of crime took place. Therefore, in the following period, the police will have to focus on the activity of perpetrators of criminal offences of premeditated murders committed with the intention to obtain property-linked benefit, to seize the benefit or find it, thus to ensure efficient confiscation of proceeds of crime.

The particularly serious crime of premeditated murder of an investigative journalist and his fiancée committed in February 2018, which also strongly affected the development of further events in Slovakia, was among the cases with the greatest media coverage. Foreign partner units and Europol also participated in the investigation into this criminal case; Threema application data was seized and extracted and it became underlying data for many other criminal prosecutions. In September 2018, four people were charged with an offence of premeditated murder, and in October 2019, a motion for indictment against the persons accused was filed. Two persons indicted were found guilty of the premeditated murder and they were sentenced to 15- and 25-years' imprisonment. In 2019, the results of evidence in this case helped clear up additional older murders from 2011 and 2016 that had not been cleared up, and preparations of premeditated murders of three prosecutors were cleared up, where five people were charged with murder preparation. The results of evidence also brought additional suspicions of criminal offences of corruption of various public officials, which are mostly under investigation today; 18 persons were charged, out of it 13 judges from various courts were actively working as judges at the time of charge.

The assessment team also paid special attention to the aspects of combating **illicit manufacturing, possession of trafficking in firearms, ammunition and explosives.**[8] Based on knowledge obtained from the results of operational and search activity and investigation in this section of criminality it should be noted that despite tightening up partially the legislation regulating the possession and sale of Flobert guns, **during the monitored period, the legal arms market in the Slovak Republic was abused by perpetrators, who easily procure expanding long and short guns without any registration or licence to possess and subsequently, they easily convert them into guns capable of shooting**. Perpetrators purchase weapons in general from legal vendors in the territory of the Slovak Republic and then, they modify them themselves or with the assistance of other people so that the guns can be used to shoot usually with 9mm cartridges, which means that a D category weapon according to Article 7 (1) (a) of the Act on Firearms and Ammunition[9] becomes A category weapon according to Article 4 (2) (g) of the quoted act. **The modified – prohibited weapons are sold by perpetrators directly or through other people for unascertained prices with profit to people from foreign organised crime, usually in the Netherlands, Italy, Belgium, France and other countries.**

Within the OTF LYNA action days in December 2019, a case was detected in cooperation with Europol (AP&WE), it was a case of **particularly serious crime of prohibited acquisition and possession of firearms and trafficking** executed within the framework of international judicial and police cooperation with the authorities of the United Kingdom, Italy, Belgium, the Netherlands, and Poland with a working title "LYNA". For the purpose of purchase of Flobert guns, their illicit reworking to functional firearms and subsequent sale on behalf of a business company with its registered office in the SR, after a previous order, members of an international organised group ensured the purchase of functional firearms, they had them converted into D type weapons – Flobert by certified manufacturing and test shops and knowing that the weapons can be and are reworked to functional firearms, they collected them for citizens of Ukraine acting under a different identity provided into the book of Flobert-type guns with a common goal to cover the real intention of handling the purchased Flobert guns. Then, the citizens of Ukraine transported the purchased firearms to an industrial building in the District of Košice, where they converted them into functional firearms without respective permit, using the procured tools; subsequently, they transported them and sold with profit to various people in the countries of Western Europe. This activity provided them with financial benefit amounting to at least EUR 152,000.00. In this case, more than 180 firearms were seized (both short and long), main parts of firearms (prohibited parts of firearms – frame, barrel, slide), various vice and metal-working fixtures, tools and parts of inserted barrels after the reactivation of firearms from a Flobert-type weapon precursor to an efficient firearm, and a great amount of smuggled goods (amber). During the monitored period, **the group committing this criminal activity purchase 1503 weapons and reworked them; the price of modifications amounted to EUR 13,950.00. With a margin of 16.25 %, this would reach a financial benefit of EUR 172,848.80, and the subsequent sale price within the Slovak Republic would amount to EUR 1,250,491.00. A hypothetic, however, really possible maximum profit in the**

[8] In terms of long-term statistical reporting and with respect to the character of the criminal offence, this type of criminal activity is included in criminal violence.
[9] Act No. 190/2003 Coll. on firearms and ammunition and on the amendment to certain acts

Netherlands could represent an amount of EUR 5,318,455.00, in the United Kingdom even EUR 8,509,528.00.

From information obtained in connection with the "LYNA" case it was obvious that the main accused person **purchased a single-family house, for which they paid in cash,** and despite the police's effort to prove the income from the above criminal activity, the accused person was not prosecuted for the legalisation of proceeds of crime because their legal activities overlapped the illicit activity, thus, evidence of legalisation would be disputable according to the Prosecutor's Office. Thus, it was not obvious which activity was at the end of the main criminal offence, from which the income had been obtained, and what it included, and where the criminal offence of legalisation of proceeds of crime started. The accused person sold a great quantity of firearms, which had not been seized yet as illegally reactivated, thus, their sale was legal. In other words, such weapons were sold for a purpose different from commission of criminal activity. In connection with the LYNA case, about 150 D Category firearms were seized, which had been with poor quality reworked from efficient firearms and could have been or should have been used for further sale and possible reactivation; a decision on the forfeiture of these firearms will be made by a competent court. The pre-trial proceedings in this criminal case (LYNA) are pending.

The report of **EUROPOL SOCTA from 2017** contains a case from 2016, when two members of the Italian mafia clan 'Ceusi' were arrested on charges of **firearms trafficking**. They had legally purchased over 160 decommissioned expansion firearms (at that time, in Slovakia, these firearms could be sold using the identity card also online, via the internet), some of the firearms were reactivated and sent to Malta or to Italy by a forwarding company. After illicit reactivation to efficient firearms, the value of the weapons increases several times on the foreign market. After the reactivation, several thousands of Euros can be obtained abroad for an expansion weapon, which cost originally hundreds of Euros. If a greater number of reactivated firearms is sold, illicit proceeds of this activity can be considerable. The Slovak police provided the Italian police with necessary collaboration in this case, and based on information provided by Slovak police authorities, other buyers were identified, who had links to Italian organised crime abroad.

It can be stated, also using the cases investigated so far as a basis, that purchases of greater quantities of these firearms by individuals but in particular by organised groups, their subsequent reactivation to efficient firearms and abuse in committing criminal violence could also represent an ML threat. Such form is then capable of generating considerable volumes of proceeds, especially when there are links to cross-border form of criminality. It results from the executed case that illegal firearms are placed and proceeds are generated in particular in EU Member States. It should be noted that if the competent institutions and the legislator adopted sufficient legislative measures in the form of more thorough record-keeping of Flobert guns (Article 7 (1) (a) of Act No. 190/2003 Coll.), as well as an accurately defined modification of such firearms from efficient firearms, the interest in purchasing them in the territory of the SR would be minimised. Both individuals and organised groups abuse gaps in the legal system of the SR, when they trade in weapon precursors and generate legal profits in the SR, while after the reactivation, these precursors are abused to generate illicit profits and commit criminal violence.

With respect to a high latency of this criminal activity, the volume of illicit trafficking in firearms and the proceeds of this activity cannot be relevantly estimated.

2.1.2. Forecast of ML threat development in criminal violence

In the next period, a stagnation or a moderate increase in criminal violence is expected. Poor economic and social situation, as well as alcohol and drugs can be considered the most important acceleration factors which will affect the development of criminal violence. Other significant acceleration factors will include unemployment, violence in media, racism and xenophobia, low penalties. The development of this criminality can be likewise affected by the global pandemic caused by the COVID-19 disease. On the contrary, experts provide factors of criminal violence weakening, such as prevention, improvement of economic situation and reduced unemployment; however, they are only considered to be probable.

In general, it can be expected that criminal violence will continue to have a marginal significance in relation to possible generation of proceeds of crime and their subsequent legalisation, without a significant change of tendency. The organised form of commission of certain types of criminal violence and trafficking in firearms, especially linked to cross-border form of criminality, should still be considered an ML threat.

2.2. Criminal offences against morality [10]

2.2.1. ML threat factors

In terms of ML threat, in particular trafficking in human beings (hereinafter "THB") has a potential to generate proceeds of crime; the proportion of unrecorded proceeds is higher than the value of detected proceeds. Taking into account this fact, the ML threat is medium-low and the trend of development without change. However, in terms of Criminal offences against morality as a whole, the proportion of ML threat in terms of unrecorded proceeds is not significant.

The occurrence of criminal offences against morality **in terms of their number is not very significant**. Their share in the overall criminality increased by 0.42 % (previously by 0.13 %) compared to previous assessment. The biggest percentage was recorded in 2019 (0.53 %) and the lowest one was recorded in 2016 (0.27%). An increase in the number of detected criminal offences against morality compared to the previous assessment was recorded **in particular for the criminal offence of dissemination of child pornography and production of child pornography**, and it **results from an increased activity of the police in the area of detection of the criminal offence of dissemination of child pornography, as well as the risk identification and measures adopted after the first round of the NRA.** On the contrary, there was a decrease in the criminal offence of pimping compared to the previous assessment. Taking into account the latency of criminal offences against morality, it is difficult to evaluate their indicators because victims often hide the consequences of the trauma caused, or there are various cases of sexual abuse. Therefore, **it is difficult to determine the accurate amount of damage caused by this criminal activity**. Because of the latency of this criminal activity, it is difficult to determine the amount of proceeds, however, according to the findings from investigation into this criminal activity,

[10] Pimping Article 367 (old Article 204), Production of child pornography Article 368 (old Article 205b), Dissemination of child pornography Article 369 (old Article 205c), Possession of child pornography Article 370 (old Article 205d), Trafficking in human beings Article 179 (old Article 246)

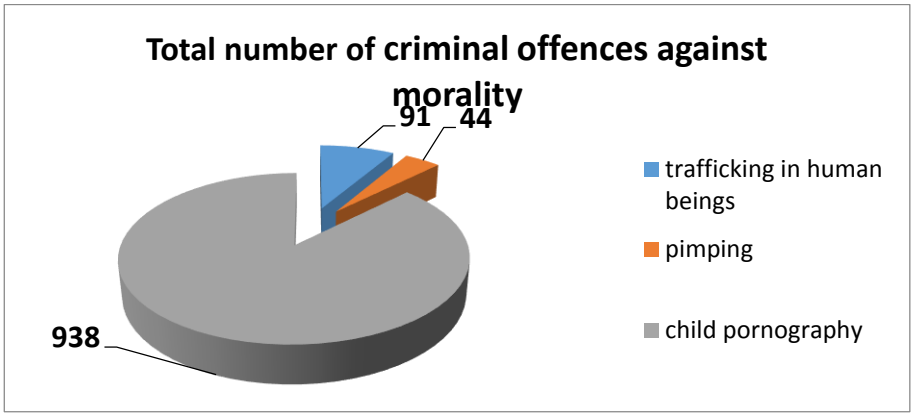
the profit/proceeds are the subject of the perpetrator's private consumption (e.g., purchase of motor vehicles, acquisition of real estate), and they are continuously spent.

For the monitored period 2016 to 2019, out of the total number of criminal offences against morality, there were 282 cases of conviction (a share of 26.28 %), and in 23 cases, the penalty of forfeiture of a thing was imposed or the protective measure of confiscation of a thing, **however, these do not cover significant volumes of proceeds of crime.**

Even despite an increased growth of criminal offences against morality compared to the previous assessment, the stabilisation of these criminal offences at the level of occurrence for the period of the previous four years is expected.

As regards the organised form of commission of criminal activity of trafficking in human beings (hereinafter THD), from 2016 to 2019, total **13 organised groups** were investigated, with the purpose of labour exploitation in four cases, forced begging in four cases, sexual exploitation in two cases, and sexual exploitation along with forced marriages in additional two cases.

The absolute majority of perpetrators were males abusing a poor social and family situation. Young people, women and children become victims of this criminal activity most frequently. In most cases, victims knew the perpetrator.



In terms of ML threats, THB is significant; it is among the most lucrative activities with an international aspect. It is carried out for various purposes, however, compared to the previous assessment, the biggest percentage belongs to sexual and labour exploitation followed by forced begging.

Within the EU, THB is among key threats, and today, it represents one of the most spread forms of international organised crime. It is a phenomenon bringing profits to its organisers that are comparable with profits from illicit trafficking in drugs or firearms.

Based on the investigation into circumstances of this type of criminal activity we can state that the financial resources obtained by the criminal activity from THB, i.e., **proceeds of crime,** are **used by** perpetrators **mostly for their own needs, both in the territory of the SR and abroad** (construction of houses in the SR, lease of houses in the UK, purchase of expensive

cars, jewellery, arrangement of doggish wedding parties and celebrations of family members). According to obtained information, currently, **proceeds generated abroad prevail, however, only very little compared to proceeds in the territory of the SR**.

With 91 cases, THB represents 8.48 % of the total number of criminal offences against morality, and 22 convictions fall on this criminal offence (a share of 24.18 %), the penalty of forfeiture of a thing was imposed in one case. No penalty of forfeiture of property or protective measure was imposed.

After assessing the statistical data for the period 2016 to 2019, we can state a significant qualitative change: the SR is not only a traditional country of origin or source country of THB victims, just as in the previous period; we also record an increase in the identified victims exploited in the SR as a target country, where the number of victims in the monitored period even exceeded the number of victims exploited in the United Kingdom of Great Britain and Northern Ireland (hereinafter "Great Britain"), which, in the long term, has been a country with the highest number of exploited Slovak victims. In 2016 to 2019, the SR was a source country in particular for Great Britain and the Federal Republic of Germany (hereinafter "Germany"), as well as other European countries.

In 2019, the first victim of THB was identified, coming from a non-EU country; it was a young woman of Afghan origin, who was sold by her own father in Iran for the purpose of forced marriage with a man of Afghan origin living in Germany. During the air transportation to Germany, the girl was identified by Slovak police authorities when entering the SR and placed in the Centre for Families and Children. The marriage itself did not take place.

In most cases, perpetrators charged with the criminal offence of THB were Slovak nationals and only seven perpetrators were foreigners (Italy, Romania, Hungary, Pakistan, Serbia, Czech Republic and Poland).

The perpetrators of the criminal offence of THB are sometimes individuals; however, more frequently they are **groups of traffickers**. Victims are usually recruited in the SR and exploited abroad or within the SR. Groups of traffickers consist either only from men or these are mixed groups of men and women. There were women as individual perpetrators in THB cases in particular for the purpose of sexual exploitation. In cases of forced begging men prevail as perpetrators. When recruiting victims, perpetrators use fraudulent conduct and trickery, when they promise the victim a well-paid job abroad. During the exploitation itself, perpetrators use various methods, from coercion and mental pressure to violent methods of coercion by locking, beating, deprivation of food, etc. Perpetrators are often from close surroundings of the victim. Depending on the person and their age, place of origin and the purpose, **the amount collected when selling a person, ranges from EUR 3,500.00 to EUR 20,000.00.**

Almost all identified THB victims in the period 2016 to 2019 were Slovak citizens (199 victims), seven foreign victims were recorded within the monitored period (Romania, Hungary, Serbia and Afghanistan). Some of the victims were exploited in several countries; therefore, the number of victims exploited in individual countries is slightly higher than the total number of identified victims.

In the area of THB, female victims continue to prevail over male victims; however, we have recorded an increased number of child victims of THB; they are exploited in particular in Slovakia. **In sexual exploitation and forced marriages**, victims are almost exclusively women; **in labour exploitation**, victims are mainly men, in THB for the purpose of **forced begging**, victims are men to a greater extent than women. Forced Roma marriages represent a new purpose of THB recorded for the first time in 2017, where victims are minor and youthful girls from the Roma community. Victims are also individuals attending special schools due to physical or mental handicaps. **The perpetrator's profit ranges from several hundred of Euros to several thousands of Euros.**

As **regards the forms of exploitation,** the situation in the SR is equal to the one in other EU countries and globally, where sexual exploitation prevails (46% of cases), followed by forced begging (19% of cases), labour exploitation (13% of cases), forced marriage (11%), and the rest were combinations of the above purposes of exploitation (11%). Some victims were also abused through several forms of THB, e.g., sexually and by being forced to contract marriage of convenience.

In detecting and investigating THB cases with an international element, the national unit cooperates in particular with the international institutions Europol and Interpol, through the seconded police staff sent to execute civil service abroad, as well as through a direct contact with police services of EU Member States interested. The system of requests for mutual legal assistance or the submission of a criminal case abroad is also utilised intensively. However, within the international cooperation, the conclusion of agreements on joint investigation teams (hereinafter the "JIT") is most practical and well-proved; they are used to facilitate investigation and criminal prosecution, obtain evidence and relevant information, and greatly contribute to successful conviction of perpetrators, to the thwarting of their activities; evidence obtained can be used for the purposes of criminal prosecution and seizure and forfeiture of proceeds of crime in both countries.

The activity of the first JIT (SVANETIA) in history was successfully finished in 2017 (the agreement for setting up the JIT was signed in 2013); Great Britain was a party to the agreement. The case concerned sexual exploitation of Slovak victims and contracting forced marriages in the territory of Great Britain with third-country nationals for the purpose of regularisation of their stay in the territory of the European Union. In 2016 – 2019, the national unit was member of other four JITs; competent units of Great Britain were a party in all of them: JIT SYNAPSIS (sexual exploitation and forced marriages of Slovak women in Great Britain) from 2016, whose activity was terminated by the Slovak party in 2018, JIT ROBOTIC (labour and sexual exploitation of Slovak victims in Great Britain) from 2017, JIT LANGSAT (labour exploitation of Slovak victims in Great Britain) from 2017, and JIT TENYCAPE (labour exploitation of Slovak nationals in Great Britain) from 2019; within the last three JITs, cooperation still continues.

In the criminal cases investigated by members of the National Unit for Combating Illegal Migration (NJBPNM) **in connection with the criminal offence of THB, financial investigation is carried out** in relevant cases, which verifies the property profile of the suspicious or accused person, in order to detect transfers of financial resources from criminal

activities and to ascertain the amount of unjust enrichment from criminal activities based on which the merits of the criminal offence were qualified.

Despite the fact that THB is a predicate criminal offence for the legalisation of proceeds of crime, the financial investigations carried out in THB cases **in the period 2016 – 2019 did not manage to obtain sufficient evidence and prove that perpetrators had obtained their property through criminal activities or from proceeds of crime, based on which criminal prosecution for the criminal offence of legalisation of proceeds of crime could have been commenced**. Within the investigated cases of trafficking in human beings, the perpetrators continuously consumed the income obtained from criminal activities to cover their costs of living and to finance their addictions (drugs, alcohol, gambling machines). As no evidence proving the acquisition of perpetrators' property or financial resources from criminal activities was obtained, proceeds within the investigated cases of the criminal offence of trafficking in human beings were not drained.

Compared to the previous assessment, a significant increase in the number of detected criminal offences in the area of **child pornography**[11] was recorded. The increase was recorded in particular for criminal offences of dissemination of child pornography and production of child pornography; there are 794 of these cases in this period. This increase also **results from an increased activity of policemen focused on detecting this criminal offence.** However, with respect to the virtual nature of this criminal activity, it is difficult to ascertain the exact number of victims and more detailed data on them. As in the previous period, girls prevail as victims of this criminal activity, boys represent a smaller share.

Out of the total number of 938 cases concerning child pornography detected in 2016 to 2019, in 225 cases, a conviction was issued (23.99 %) and in 19 cases, the penalty of forfeiture of a thing or a protective measure was imposed, thus, the instruments used to commit this criminal activity were confiscated.

In some cases, the criminal offences of child pornography may occur concurrently with one or more other criminal offences, mostly from among criminal offences against morality and criminal violence[12].

Despite the fact that the clear-up rate is not high, compared to other types of criminal offences, the fact that in this criminal activity it is possible to carry out a very efficient retrospective investigation because the process of creation and storage of digital tracks is different from other, for example, biological traces or shoeprints (in this case, the track is de facto indestructible because any activities leading to its removal allow the creation of other tracks) can be considered a positive aspect. If a perpetrator uses technical means to conceal their identity or activity (e.g. anonymous proxies), once having been revealed, this fact becomes an aggravating circumstance.

[11] Production of child pornography Article368 (old Article 205b), Dissemination of child pornography Article 369 (old Article 205c), Possession of child pornography and participation in child pornographic performance Article 370 (old Article 205d)

[12] Bodily harm (Article155, Article156, Article157), Illicit distribution of drugs (Article174), Serving alcoholic beverages to minors (Article175), Extortion (Article189), Duress (Article192) etc.

It is exactly the area of dissemination of pornography, where the internet as a source of communication brought possibilities of more efficient and faster dissemination with the preservation of a great amount of anonymity, thus hindering the work of law enforcement authorities.

With respect to the character of child pornography, damage amounting to EUR 83,000.00 was ascertained for the assessed period; however, it can be assumed that the volume of perpetrators' proceeds is higher.

Out of the criminal offences of child pornography, the criminal offence of dissemination of child pornography represents a medium-low ML threat with an upward trend because it is difficult to estimate the expected amount of unrecorded proceeds, however, it is definitely higher than in the reported crime.

2.2.2. Forecast of ML threat development in criminal offences against morality

In general, it can be stated that there is a gradual increase in the detected criminal offences against morality, and in the next period, stabilisation of these criminal offences is expected at the level of average occurrence for the period of last four years or a moderately rising trend. Mass media promoting violence and dysfunctional families are the most important acceleration factors of criminal offences against morality, which will probably take place in the following years. The development of this criminality can be likewise affected by the global pandemic caused by the COVID-19 disease. However, criminal offences against morality will continue to be a small-share category of criminality.

An increase in the commercially motivated criminal activity (pimping, THB), which is a source of illicit proceeds, will represent the highest rate of ML threat from this type of criminality. The influence and importance of the internet as an important factor of ML threat for the expansion of criminal offences against morality will continue to grow.

The THB itself and its latency is also affected by the international character of this criminality, lack of willingness of victims to cooperate with competent authorities, lack of evidence convicting traffickers in human beings, as well as the variety of data collection methodologies and THB definition itself in individual countries.

2.3. Criminal offences against property[13]

2.3.1. ML threat factors

In assessing criminal offences against property, it was found out that in terms of ML threat, the criminal offence of theft still has the highest potential to generate proceeds; its

[13] Theft Article 212 (old Article 247), Failure to pay wages and redundancy payment Article 214 (old Article 248a), Unlawful enjoyment of a thing of another Article 215 (old Article 249)

assumed amount of unrecorded proceeds is slightly higher, the ML threat is medium-low with a downward trend.

The criminal offences of failure to pay wages and redundancy payment and of unlawful enjoyment of a thing of another represent a low ML threat with a downward trend.

In terms of assumed amount of unrecorded proceeds in these criminal offences we can state that the proportion of the amount of unrecorded proceeds is not significant. The ML threat in criminal offences against property as such is medium-low with a downward trend.

As in the previous assessment, criminal offences against property constantly occupy a dominant position in the general composition of criminality, both in the number of committed criminal offences and in the number of prosecuted persons. The number of prosecuted persons, however, despite the dominant position, has a **most significantly decreasing tendency** (from 15,038 cases in 2019 to 22,414 cases in 2016). Compared to the previous assessment, there was a significant decrease in criminal offences against property (162,396 cases in the previous assessment). **The percentage of prosecuted persons in total exceeds one half, i.e., 55.42 %** with a stabilised tendency.

The decrease in criminal offences against property is not so much ensured by the entities responsible for control, it is rather supported by potential victims. Citizens behaving ever more responsibly provide fewer opportunities to perpetrators. In addition to an improved technical level of protection of property, insurance companies are also more cautious in verifying fictitious thefts.

In the monitored period of the years 2016 to 2019, out of the total number of 77,278 criminal offences against property, there were 21,044 convictions (27.23 %), in 23 cases, the penalty of forfeiture of a thing was imposed, in four cases the penalty of forfeiture of property, and in six cases, the protective measure of confiscation of a thing was imposed.

The damage caused by criminal offences against property, thus, also the potential volume of proceeds of crime in the monitored period amounts to EUR 164,052,000.00, it is a considerable decrease compared to the previous assessment amounting to EUR 597,174,000.00. In individual years, the damage caused ranged from EUR 33,309,000.00 (2019) to EUR 47,124,000.00 (2017), i.e., the damage caused by criminal offences against property has a decreasing tendency by 29.32 %. The damage ascertained within criminal offences against property represents 5.97% of the damage ascertained in overall criminality in the monitored period.

The profits or proceeds from criminal offences against property **are to a great extent the subject of the perpetrator's private consumption.**

As in the previous assessment, the factors affecting criminal offences against property include:

- unemployment resulting in lack of resources for the basic necessities of life,
- decreased standard of living, poor social and life economic conditions,

- drug addiction,
- persisting lack of willingness of citizens to cooperate with the police.

As regards territory, thefts are committed in particular in large cities, where there is a greater concentration of objects of interest of perpetrators, as well as greater anonymity in comparison with the rural environment. In many cases, inattention and carefree approach to people's own things play a great role.

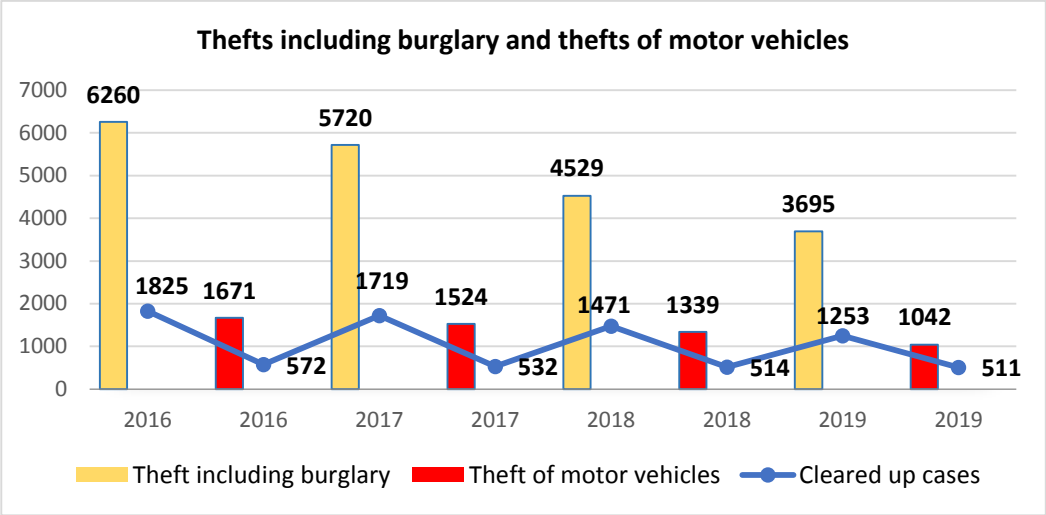
Thefts of high-value things, in particular motor vehicles and machines, which persist in the long term, have a special importance in relation to the issue ML threats. There is also an organised form of this criminal activity, in particular in stealing goods transported by freight road transport, as well as in the area of flat and recreational structure burglaries.

As regards the way of commission of criminal offences of theft, **burglary** prevails, mostly in the form of violent overcoming of the securing obstacles (breaking open the windows, doors, breaking the windows, breaking the locks), **however, the forms characterised by a more sophisticated approach with the use of specially modified burglars' tools were identified only in a few isolated cases**. In terms of the amount of caused damage and frequency of recorded occurrence, thefts including burglary are among serious and most frequently committed criminal offences against property.

Compared to the previous assessment, there was a significant decrease in the number of thefts including burglary from 52,195 cases to 20,204 cases.

Thefts of motor vehicles (hereinafter "MV") form a separate category; they are committed mostly in bigger towns. **The number of detected cases, as well as the clear-up rate has dropped compared to the previous assessment**. The adoption of measures, such as **originality check**, connection of the SR to the information system of record-keeping of drivers and vehicles EUCARIS (interconnection of national records of vehicles), control of fictitious imports, as well as **a significant increase in the international police cooperation within national contact points for car criminality CARPOL** contributed to the decrease in the number of thefts of MV.

MV theft perpetrators are mostly well-organised groups equipped with the state-of-the-art electronic devices (e.g., GSM and GPS signal jamming) having knowledge of MV anti-theft devices and the ways of bypassing them, of the location of identifiers and the way of falsification of MV documents. Most frequently, stolen MV are dismantled for spare parts. Cases were recorded with an increase in the number of legalised vehicles, which had been stolen abroad and after legalisation, they had been returned to the used car market within the countries of the European Union. On a large scale, stolen vehicles were imported to Slovakia, the identity was changed and legalisation was carried out with authentic blank documents, falsified vehicle documents and authentic documents of fully damaged and destroyed vehicles. Legalisation was also confirmed by originality check stations, where modus operandi is based on the principle of loyal persons working at originality check stations, who, for cash, designated a modified vehicle as a vehicle in good order but it was a vehicle with modified identifiers and had been acquired during criminal activity.



Petty thefts in shops qualified pursuant to Article 212 (2) (g) of the Criminal Code represent a part of detected thefts. This criminal activity is committed by people at the margins of society who procure food, cigarettes and alcohol in such a way. A high degree of recidivism is recorded among the perpetrators of this criminal offence. The application of the above provision, which has lasted several years, did not contribute to reduction in petty thefts in shops. This provision did not dissuade the persons previously penalised for the delinquency from further unlawful conduct despite the fact that under certain circumstances ("has been sanctioned for such offence in the past twelve months") they can be liable to a term of imprisonment of up to two years.

The above unlawful conduct has almost no potential of ML threat, does not generate income which could be the subject of legalisation of proceeds of crime. However, the above provision of the Criminal Code disproportionally burdens law enforcement authorities and courts and consumes resources which could be otherwise used for investigation and criminal prosecution of serious criminal activities.

Criminal offences based on **fraudulent conduct[14] with 11,053 cases** represent a great share of criminal offences against property with a potential of ML threat, however, with respect to their **character, they are classified into criminal offences of economic nature (22.85 % of the total occurrence of criminal offences of economic nature**, more details in Chapter 2.4.). The total damage caused by the above criminal offences in the monitored period amounts to EUR 314,552,000.00, which means **11.45 % of the total damage**. In this area, too, there was a decrease in the damage caused by EUR 364,813,000.00, which means 46.30 % compared to the previous assessment.

[14] Fraud Article 221 (old Article 250), Credit fraud Article 222 (old Article 250a), Insurance fraud Article 223 (old Article 250c), Subsidy fraud Article 225 (old Article 250b), Unjust enrichment Article 226 (old Article 250d), Fraudulent bankruptcy Article 227 (old Article 250e), Induced bankruptcy Article 228 (old Article 250f)

2.3.2. Forecast of ML threat development in criminal offences against property

In terms of ML threat potential, only some types of criminal offences against property have the potential to generate proceeds of crime. Based on the team's analysis, these are mainly thefts of high-value things.

In the next years, too, criminal offences against property will represent the most frequent type of criminal activity, which will be accompanied by a relatively low clear-up rate of these criminal offences. A high level of unreported criminal offences against property will also persist. Therefore, any further drop in registered criminal offences against property need not mean that their state really decreased.

Main acceleration factors, which will probably and significantly affect the development of criminal offences against property in the next years, include: economic and social situation, drugs and alcohol, unemployment and low protection of private property. This also implies that in terms of type and volume of generated proceeds of crime, these will be mostly things of immediate consumption; thus, these things will not bring significant stimuli for sophisticated legalisation moments and jeopardise the functioning of the market economy.

The most important factors in decreasing the criminal offences against property in the next years include in particular the strengthening of prevention (moderately more probable) and repression (moderately more significant), reduction in unemployment and improved protection of property.

Taking into account that persistence of a higher rate of latency in criminal offences against property is expected, the threat of legalisation of proceeds of this type of criminal activity will be at the same level as so far or will have a slightly accelerating trend.

2.4. Criminal offences of economic nature [15]

2.4.1. ML threat factors

In terms of overall criminal offences of economic nature, we can speak about a medium-high threat with a sustainable tendency of threat level, where the assumed amount of unrecorded proceeds is (disproportionately) higher.

Although perpetrators of criminal offences of economic nature are in general interested in profit, in terms of ML threat, it is not a homogeneous criminality. **Only some criminal offences have the potential to generate significant proceeds with the need of subsequent legalisation,** in particular:

- tax crime, in particular:

a) tax and insurance premium evasion (**high threat**, downward trend, the proportion of unrecorded proceeds is higher),

b) failure to pay tax and insurance premium (**medium-high threat**, unchanged trend, the proportion of unrecorded proceeds is higher), and

[15] Embezzlement Article 213 (old Article 248), Unlawful manufacturing and enjoyment of payment means, electronic money or other payment card Article 219 (old Article 249c), Fraud Article 221 (old Article 250), Credit fraud Article 222 (old Article 250a), Insurance fraud Article 223 (old Article 250c), Subsidy fraud Article 225 (old Article 250b), Unjust enrichment Article 226 (old Article 250d), Fraudulent bankruptcy Article 227 (old Article 250e), Induced bankruptcy Article 228 (old Article 250f), Usury Article 235 (old Article 253), Forgery, fraudulent alteration and illicit manufacturing of money and securities Article 270 (old Article 140), Tax and insurance premium evasion Article 276 (old Article 148), Failure to pay tax and insurance premium Article 277 (old Article 148a), Tax fraud Article 277a, Failure to pay tax and insurance premium Article 278 (old Article 148b), Counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark Article 352 (old Article 176), Abusing participation in economic competition Article 250 (old Article 149), Unlawful business activity Article 251 (old Article 118), Unlawful employment Article 251a, Unlawful trading in foreign currency and providing foreign-exchange services Article 252 (old Article 118a), Breach of regulations governing imports and exports of goods Article 254 (old Article 124), Breach of regulations governing the handling of controlled goods and technologies Articles 255 (old Article 124a), 256 (old Article 124b), 257 (old Article 124c), Distortion of data in financial and commercial records Article 259 (old Article 125), Damaging the European Communities' financial interests Article 261 (old Article 126), Endangering trade, bank, postal, telecommunication and tax secrets Article 264 (old Article 122), Insider trading Article 265 (old Article 128), Contrivance in public procurement and public auction Articles 266 (old Article 128a), 267 (old Article 128b), 268 (old Article 128c), Harm caused to a consumer Article 269 (old Article 121), Unfair trade practices Article 269a

- certain types of fraudulent acts, in particular:

a) MTIC frauds (**medium-high threat**, upward trend, the proportion of unrecorded proceeds is higher),

b) CEO frauds (**medium-high threat**, unchanged trend, the proportion of unrecorded proceeds is higher),

c) subsidy fraud and fraudulent bankruptcy (**medium-high threat**, downward trend, the proportion of unrecorded proceeds is substantially higher).

The following represents a special ML threat:

- Distortion of data in financial and commercial records (medium threat, unchanged trend, the proportion of unrecorded proceeds is higher),
- Damaging the European Communities' financial interests and Contrivance in public procurement and public auction (medium threat, upward trend, the proportion of unrecorded proceeds is slightly higher).

Abuse of schemes of legal persons is an important aspect of predicate criminal offences of economic nature with a significant level of ML threat with an unchanged trend; the mechanism of their abuse continues to develop and transform itself which represents a special challenge for AML/CFT entities.

As in the previous assessment, criminal offences of economic nature represent the second most extensive group of criminality in terms of the number of detected criminal offences. They are characterised by a high latency, with often large profits obtained by perpetrators, much higher than for criminal offences against property.

In criminal offences of economic nature, proceeds generated in the territory of the SR prevail; they are either invested within financial markets or in real estate, cars and for personal consumption.

As regards the qualitative aspect, it is necessary to note a rising trend of the volume of detection and prosecution of carousel frauds and related abuse of sophisticated schemes of legal persons with cross-border generation of proceeds of crime.

In the monitored period 2016 to 2019, out of the total number of 48,381 criminal offences of economic nature, there were 11,125 convictions (22.99 %), **and in 56 cases, the penalty of forfeiture of a thing was imposed**, **in nine cases the penalty of forfeiture of property, and in 14 cases, the protective measure of confiscation of a thing was imposed, which represents a positive increase compared to the previous period.**

Compared to the previous assessment, there was an increase in the total damage caused by criminal offences of economic nature by EUR 410,091,000.00 to EUR 2,032,443,000.00, which represents 73.98 % of the total damage. In individual years, the damage ranged from EUR 207,811,000.00 in 2018 to EUR 249,089,000.00 in 2019. However, in 2017, one specific case of distortion of data in financial and commercial records pursuant to Article 259 of the

Criminal Code was detected, with damage amounting to EUR 1,118,675,000.00, for that reason damage in 2017 amounted to EUR 1,425,195,000.00. As in the previous assessment, tax criminal offences and frauds represent the highest share of this criminality.

It results from the assessment of individual years that the amount of damage caused by criminal offences of economic nature represents a high potential of ML threat in particular when considering the clear-up rate of criminal offences of economic nature, which ranged from 48.42 % to 52.95 %.

Year	Number of detected criminal offences of economic nature	Number of cases clarified	Clear-up rate in percent	Damage caused by criminal offences of economic nature in thous. EUR	Share in the overall criminality in percent
2016	12,927	6,259	48.42	247,094	21.39
2017	12,632	6,375	50.47	1 328 449*[16]	21.84
2018	11,539	5,974	51.77	207,811	22.01
2019	11,283	5,974	52.95	249,089	22.65
Total	48,381	24,582	50.81	2,032,443	21.95

The perpetrators of criminal offences of economic nature were motivated by obtaining financial resources through:

- a failure to fulfil tax and levy liabilities by business entities,
- abuse of payment means to withdraw cash from ATMs or during cashless payments,
- abuse of financial resources made available to them for their own purposes,
- unauthorised receipt of social security benefits, and
- a failure to pay pecuniary claims to employees.

Compared to the previous assessment it can be stated that criminal offences of economic nature have had a long-term **trend of gradual decrease in the number of detected criminal offences, with a positive aspect of gradual increase in the clear-up rate.** Despite these facts it can be expected, the **unrecorded cases as well as proceeds are (disproportionally) higher than detected cases and proceeds of this criminality (high rate of latency).**

As in the previous assessment, perpetrators of criminal offences of economic nature were people with higher education – secondary schools and universities, or these people managed the so-called executors. These managing persons **use sophisticated methods of commission and concealment of criminal offences of economic nature.**

[16]In 2017, a specific case (the above mentioned one) of distortion of data in financial and commercial records pursuant to Article 259 of the Criminal Code was detected, with damage incurred that amounted to EUR 1,118,675,000.00.

Often, in particular in the cases, in which such criminal activities cause high damage, **straw men** are used in committing criminal offences. These are in particular the cases, when a business company does not fulfil its tax and levy liabilities or it performs its business relationships in such a way that it does not record its income in the company, subsequently, a partner transfers their business share to a straw man, who also confirms the take-over of accounting and tax records although it does not really happen. Subsequently, the former partner acts in a new company with similar or identical objects of the company and **uses finances acquired by unlawful activities** in the first company **for the personal use**.

Proving the subjective aspect of the criminal offence in the above criminal offences **is very difficult and time-consuming**. Documentary evidence (e.g., accounting and tax documents, tax returns, audit protocols, various permits and licences), professional and expert opinions represent main evidence in criminal offences of economic nature. Criminal proceedings depend on the provision and assessment of the above evidence.

In particular due to the absence of documentary evidence and proactive parallel investigation, in the cases with the use of straw men, the documenting of criminal activities is very difficult, and in general, the beneficial owner is not criminally punishable, which represents an extraordinary potential of ML threat.

As in the previous assessment, in the monitored period, frauds in freight transport of goods with an immanent cross-border character were also detected.

It is difficult to estimate the volume of proceeds generated by frauds in international freight transport, however, it represents a higher rate compared to reported criminal activity; in this context, it means a significant potential of ML threat with a stabilised or slightly decreasing tendency.[17]

The modus operandi of frauds in transport consists in pretending that transport of goods will be carried out from one place to another in various countries of the EU by trucks; however, after the goods have been loaded, they are not delivered, and the goods along with the truck vanish into thin air. In these criminal activities, perpetrators in various ways conceal the real identity of people performing and organising the transport and often even the genuine origin of trucks. The perpetrators, who register to goods transport performance, hide behind **non-existing business entities or business entities established formally in EU countries, which do not carry out any real business activity, and the persons acting officially in the bodies of the companies are straw men**. The perpetrators also mask their false intention to perform proper transportation of goods by submitting **forged documents** necessary for goods transportation in international freight transport.

[17] The measures adopted in the assessed period already reflect the risk

2.4.2. Tax criminal offences

As in the previous assessment period, criminal offences of economic nature recorded most frequently were **tax criminal offences.**[18]

ML threat for tax crime is medium-high to high. The expected amount of unrecorded proceeds or the volume of benefit obtained is disproportionately higher than for reported criminal activities. The trend of ML threat is without any change, except for the criminal offence of failure to pay tax and insurance premium, whose tendency is slightly rising.

Compared to the previous assessment period, in the period from 2016 to 2019, there was a slight decrease in the number of tax criminal offences and amount of damage caused. In 2016 to 2019, 21,901 tax criminal offences were detected in total, of which 15,339 were cleared up (70.04 %). In relation to overall criminality, tax criminal offences represented a share of 8.55 %, and **damage amounting to EUR 512,188,000.00** was caused to the state budget**, which represents 18.64% of the total damage within the prosecuted criminality.** The occurrence of tax criminal offences represents **45.27% of criminal offences of economic nature**.

More efficient procedures of law enforcement authorities (improved quality of evidence), and more efficient detection of tax criminal offences (e.g., through VAT control statement which is an invaluable source of information for law enforcement authorities) contributed to the decrease in this type of criminal activity. These factors affect probably the less sophisticated perpetrators who are not as dangerous as large organised groups of tax criminals also operating in several States.

In the monitored period, out of the total number of tax criminal offences, there were 2,517 cases of convictions (a share of 11.49 %), in eight cases, the penalty of forfeiture of a thing was imposed, in six cases, the penalty of forfeiture of property was imposed and in two cases, the protective measures of confiscation of a thing.

It results from the statistics of individual years that the share of tax criminal offences in criminal offences of economic nature had a rising tendency; the highest increase was recorded in 2019 (a share of 49.61 %), and the lowest one in 2016 (a share of 42.31 %).

In 2018, in pre-trial proceedings of one criminal case connected with tax criminal activities, the prosecutor of the Regional Prosecutor's Office Košice seized the whole property of two accused persons, as well as the property, which will be acquired by these accused persons after the seizure, using the procedure pursuant to Article 425 (1) of the Code of Criminal Procedure referring to the provision of Article 426 (1) of the Code of Criminal Procedure (taking into account the nature and gravity of the act and the status of the accused persons, the imposition of the penalty of forfeiture of property should be expected).

[18] Tax and insurance premium evasion Article 276 (old Article 148) of the Criminal Code, Failure to pay tax and insurance premium Article 277 (old Article 148a) of the Criminal Code, Failure to pay tax Article 278 (old Article 148b) of the Criminal Code, and after the introduction, the criminal offence of Tax fraud Article 277a of the Criminal Code

Tax criminal activities are mostly seen in the area of indirect taxes, particularly the value added tax (hereinafter "VAT"). VAT is the most important source of income of the state budget and the second most important source of income of general government. **MTIC frauds (missing trader) leading to a failure to fulfil the tax liability, manipulation/abuse of the VAT system and finally to making proper VAT collection in the State impossible represent the most serious form of tax criminal activities**.

In tax criminal offences, the main modus operandi is the accounting of **fictitious invoices**, overvalued or undervalued invoices, i.e., a way of reducing the tax liability and avoiding payment of tax fees.

Carousel frauds are the most dangerous form of MTIC frauds; they represent a permanent ML threat with a rising trend.

In carousel frauds, the state of qualified forms of criminal activities persists, when organised and criminal groups focus on committing criminal offences related to application of excess VAT deductions through special-purpose chains of business companies, whose statutory representatives are straw men controlled by the perpetrators. The manner of commission of this type of tax criminal activities is virtually not changing, i.e., the creation of company chains across several EU Member States (missing traders, buffer companies, beneficial owners, international buffer companies), use of straw men (Slovak nationals, nationals of other EU Member States), declaration of IC acquisition and delivery of goods/services within several EU States, involvement of such companies in chain or carousel frauds with VAT for the purpose of either unauthorised withdrawal of excess VAT deductions or – currently in the vast majority of cases – tax liability evasion by unauthorised deduction of VAT by large "renown" entities making real business to the detriment of state budgets of several Member States of the EU. The perpetrators fully utilise the advantages of the EU single market, i.e., free uncontrolled movement of goods and services within the EU. Mostly it concerns the circulation of goods which are small, easily relocatable, with minimum storage demands and of high value[19].

Number of investigations of MTIC frauds in the assessed period:

Period	Number of commenced criminal proceedings	Number of charges	Number of accused persons	Scope of consequence
2016	43	172	106	EUR 91,137,927.00
2017	36	38	178	EUR 49,741,186.00
2018	44	48	98	EUR 30,153,569.00
2019	37	22	80	EUR 34,680,600.00

[19] The analysis of some cases investigated by the FACO identified the following commodities: milk, energy drinks, sugar, edible oil, marble, steel, cement, scrap metal

The documented cases concerned in particular the declaration of IC acquisition and delivery of goods within the V4 countries (Czech Republic, Poland, Slovakia, and Hungary), countries such as Germany, Romania also occurred to a smaller extent. As regards the geographic division of Slovakia, the border regions with Hungary (the south of Slovakia) and with Poland hold a specific position in committing tax criminal activities. This implies that the tax criminal offences have a multinational character, as organisers of such frauds often include foreign nationals, whose examination requires international judicial cooperation in the form of legal assistance from abroad, which considerably affects the length of criminal proceedings, and in the majority of these criminal offences, it causes considerable delays in clarifying the case regarding the scope of cases, as well as the number of accused persons.

Another significant form of committing criminal activity with a considerable potential of ML threat consists in **withdrawing excess deductions of VAT.**

Commission of this criminal activity consists in producing false supplier invoices issued on behalf of business companies controlled by the perpetrators, usually ***for fictive supplies of construction work and services*** in various financial volumes according to the requirements of statutory representatives of various business entities for the purpose of accounting such false invoices in their accounting records as expenditures for the achievement and maintenance of proceeds. The objective is to fraudulently reduce the base of assessment of VAT and corporate income tax. After receiving the false invoices, the statutory representatives of these business entities perform cashless settlement of the invoices to bank accounts of the companies controlled by a member of the group, on behalf of which the invoices were issued, and they withdraw the remitted amounts (proceeds) for the settlement of the false invoices from the bank account and hand them over back to the statutory representatives of the business entities, who, according to an agreement, pay a part of the financial resources in cash usually amounting to 10 to 20 % of the value of fictive taxable payment as a reward to group members.

Detecting tax evasions is complicated because of a high rate of latency. In the conditions of the SR, the Institute for Financial Policy determines latent VAT evasions, describes the methodology of estimating VAT gap. The loss of state budget income can be approximately determined by estimating**. As estimated, in 2018, the VAT gap reached a value of 26.9% of potential VAT in the SR. Compared to 2012, when the VAT reached its peak of 40.3%, it has been reduced by more than one third**. In nominal values, the difference between the potential and real VAT proceeds in 2018 amounted to EUR 2.3 bn. (2.6% of GDP).

The perpetrators of tax frauds include both organised groups and individuals, who, in some cases, use the untaxed money (proceeds of crime) as a source for bribes to obtain public contracts, European funds, to purchase public property or illegally obtain other advantages, usually from the public sector or local governments.

After the legislation concerning tax administration had been amended, the number of cases of **special-purpose mergers of companies** with the objective to evade tax liabilities increased. In such cases, **straw men coming mostly from the neighbouring countries** act in the statutory bodies and as owners; they act according to the instructions of real owners.

Legalisation through a **network of companies abroad** is among the methods of laundering financial resources illegally obtained from tax and credit frauds and from other

criminal offences of economic nature in large volumes. Money is transferred using fictitious business transactions at first to accounts of these foreign companies, and then to the **accounts of letter-box companies in offshore countries**, which are owned or managed by organisers of criminal activities of economic nature. Then, the funds from letter-box companies are transferred to a network of accounts of other foreign companies, and from them they are probably returned back to fraud organisers as already legalised resources for the purchase of property or legal foreign business investments.

2.4.2.1. Impact of the adopted measures – "Tax Cobra"

The ever more sophisticated methods of commission of tax criminal activities affect the process of their detection, which is closely connected with the demands for taking of evidence requiring in particular time-consuming expert taking of evidence, without which it is often not possible to clarify sufficiently the facts of the case to an extent necessary for the charging of a particular person.

This hindered process was the reason for the adoption of measures focused on the provision of a joint and efficient procedure of law enforcement authorities with the Financial Administration, FACO and financial police. These are mainly interministerial meetings at central and regional levels, and use of expert consultants.

The systematic approach in combating tax criminal activities is based on the **Action Plan to Combat Tax Frauds (hereinafter the "Action Plan").** In the period from 2016 to 2019, new control mechanisms adopted by the Financial Administration and strong cooperation of law enforcement authorities contributed to considerable prevention of unauthorised payment of excess VAT deductions and imposition of tax liability.

Summary of requested excess deductions and unpaid excess deductions from the data of the Financial Administration:

Year	Finding in total in EUR	Unpaid excess deductions in EUR
2016	EUR 125,852,169.10	EUR 10,410,212.16
2017	EUR 97,289,499.36	EUR 5,640,895.66
2018	EUR 99,153,719.50	EUR 3,345,844.99
2019	EUR 77,924,125.80	EUR 854,422.37
Total	EUR 400,219,513.76	EUR 20,251,375.18

The Action Plan measures implemented and Action Plan updates focused on VAT allowed reducing the volume of tax evasions in this area and also set high-quality preventive effects.

The **establishment of JACK, the interministerial analytical centre,** with the objective to provide data between the FA and PF in case of suspect entities is among the measures (Measure No. 6) of the Action Plan.

In connection with the fulfilment of tasks resulting from the Action Plan, based on a Government Resolution of the SR, the project of cooperation between the Police Force of the SR, Financial Directorate of the SR and General Prosecutor's Office of the SR, the so-called **"Tax Cobra"** was initiated in 2012. It is a special unit of the above entities with a national competence, whose purpose is to prevent business entities from committing serious tax criminal activities, quickly exchange respective information and **analyse risks through specialised software already during the tax proceedings in connection with the verification of eligibility of a particular excess deduction of VAT by a particular tax entity.**

The success of "Tax Cobra" implementation is also proved by the data informing that from 1 January 2012 (date of Tax Cobra establishment) to 31 December 2019, the financial finding from completed tax audits amounted to EUR 984,820,130.99, out of which the unpaid excess deduction of VAT amounted to EUR 88,320,035.00. The cases included mainly **frauds with commodities such as stone, crude oil, concrete steel, non-ferrous metals, cereals, sugar, meat, timber, wine**.

The results of the Tax Cobra project present its justness and high efficiency, and success in executed cases, with the efficiency of tax audits of 91.13%.

Summary of "Tax Cobra" activity from its establishment to 31 December 2019 based on the statistical data collected by the police:

	Number of cases	Number of accused persons	Damage in EUR	Saved financial resources in EUR	Detention	Final judgement	
						Qualification	Sentence
2012 - 2019 total	**95**	**531**	**539,192,303.25**	**88,320,035.00**	**50**	**Article 277 Failure to pay tax and insurance premium**	**Prison sentence 2x7y., 1x5y., 1x3y., Suspended prison sentence 3y./5y., prison sentence 12y. + fin.penalty EUR 30,000 + ban on doing business 10y. + confiscation of an amount of EUR 1,800,000**

Recently, tax criminal activities have been recorded, which mean a transition from tax frauds in the form of unauthorised refund of excess VAT deduction to the so-called consolidation of tax liability and to frauds with electronic cash registers by unauthorised modifications of their software.

Controls based on the digitalisation of accounting documentation and introduction of the duty to back up and hand over the accounting documentation in electronic form to competent Financial Administration authorities could help increase the rate of success in detecting and proving tax criminal activities. These measures in connection with control activities performed by tax authorities could efficiently help detect tax criminal activities and infer criminal liability.

2.4.3. Other types of criminal offences of economic nature with a significant potential of ML threat

The most frequently committed criminal offences with a potential of ML threat, whose nature causes their classification into criminal offences of economic nature[20] include the criminal offence of **distortion of data in financial and commercial records** pursuant to Article 259 of the Criminal Code and the criminal offence of **damaging the European Communities' financial interests** pursuant to Article 261 of the Criminal Code.

For the criminal offence of distortion of data in financial and commercial records, the **ML threat is medium with a stable trend.**

For the criminal offence of distortion of data in financial and commercial records, there was a significant decrease by 320 cases compared to the previous assessment period. During the monitored period from 2016 to 2019, 284 cases in total were detected, which means 0.59 % of the overall criminal offences of economic nature. On the contrary, the damage increased by EUR 109,558,000.00 as in 2017, one specific case of distortion of data in financial and commercial records pursuant to Article 259 of the Criminal Code was detected. This case was connected with the eligibility of accounting of reserves and contributions to the National Nuclear Fund of the SR and the damage caused amounted to EUR 1,118,675,000.00. Based on this case, the total damage caused by the criminal offence of distortion of data in financial and commercial records for the monitored period 2016 to 2019 amounted to EUR 1,127,241,000.00.

As in the previous assessment period, the criminal offence of distortion of data in financial and commercial records included cases, when perpetrators pretended to tax or other control authorities that they did not have certain documents at all or they had placed or hidden them at a place where they were not available to the authorities using common means.

For damaging the European Communities' financial interests, the ML threat is medium with an upward trend.

As in the previous assessment period, this criminal activity was focused in particular on **minor EU funds** for the support of employment, within which false and mendacious documents were submitted to the grantor of contribution in order to obtain a contribution, which was used for another purpose. In these cases, perpetrators were mainly from excluded communities, with

[20] Abusing participation in economic competition Article 250 (old Article 149), Unlawful business activity Article 251 (old Article 118), Unlawful employment Article 251a, Unlawful trading in foreign currency and providing foreign-exchange services Article 252 (old Article 118a), Breach of regulations governing imports and exports of goods Article 254 (old Article 124), Breach of regulations governing the handling of controlled goods and technologies Articles 255 (old Article 124a), 256 (old Article 124b), 257 (old Article 124c), Distortion of data in financial and commercial records Article 259 (old Article 125), Damaging the European Communities' financial interests Articles 261 (old Article 126), Endangering trade, bank, postal, telecommunication and tax secrets Article 264 (old Article 122), Insider trading Article 265 (old Article 128), Contrivance in public procurement and public auction Articles 266 (old Article 128a), 267 (old Article 128b), 268 (old Article 128c), Harm caused to a consumer Article 269 (old Article 121), Unfair trade practices Article 269a

low education, etc., who try to solve their poor financial situation in such a way. There were also cases, when after obtaining the contribution, the perpetrators did not carry out the activity and left the territory of the SR.

Another group in this area of criminal offences consists of the cases committed by representatives of business companies in a sophisticated manner, with corruption elements in order to obtain unauthorised proceeds.

This group also includes wrongly received subsidies either from funds of the European Communities or from the state budget, for the purchase of medical instruments and devices, or agricultural subsidies.

In the cases with purchase of medical instruments and devices, disproportional overcharging of purchased medical technology was detected; in this case, there is also a suspicion of the criminal offence of contrivance in public procurement and public auction pursuant to Article 266 of the Criminal Code.

In connection with the drawing of agricultural subsidies and related corruption and legalisation of proceeds of crime (the case "Dobytkár" - Stockman), since 8 October 2019 when criminal prosecution was commenced, there has been extensive investigation into the criminal offence of receiving a bribe pursuant to Article 329 (1), (2), (3) of the Criminal Code committed with accomplices pursuant to Article 20 of the Criminal Code and a particularly serious crime of legalisation of proceeds of crime pursuant to Article 233 (1) (a), (4) (a) of the Criminal Code at a stage of preparation pursuant to Article 13 (1) of the Criminal Code in connection with the provision of a non-repayable financial contribution provided through the Agricultural Paying Agency within the Rural Development Programme of the Slovak Republic. A group of individuals, which created a corruption scheme in connection with the provision of a non-repayable financial contribution provided through the Agricultural Paying Agency operated in the territory of the SR in 2015-2020; subsequently, this group of individuals also created a **legalisation scheme through contracts for work**, which solely should have concealed the origin of the proceeds of corruption crime and the proceeds could have ranged from 15 to 25% of the total volume of subsidies provided.

After the commencement of the criminal prosecution, an **extensive financial investigation was carried out**, based on which, from 3 March 2020 to 2 July 2020, six interventions within the DOBYTKÁR (STOCKMAN) action took place, with 27 natural persons detained. Subsequently, the investigator of the PF in his resolutions charged in total 10 natural persons and five legal persons with a particularly serious crime of receiving a bribe pursuant to Article 329 (1), (2), (3) of the Criminal Code committed with accomplices pursuant to Article 20 of the Criminal Code, and a particularly serious crime of legalisation of proceeds of crime pursuant to Article 233 (1) (a), (4) (a) of the Criminal Code at a stage of preparation pursuant to Article 13 (1) of the Criminal Code. Of the above number, three natural persons and two legal persons were also charged with a completed particularly serious crime of legalisation of proceeds of crime pursuant to Article 233 (1) (a), (4) (a) of the Criminal Code. Except for one person, all the accused persons were prosecuted in detention.

The total amount of bribes received by the accused persons amounts to about EUR 8,000,000.00, and the total amount of financial resources related to legalisation of proceeds of crime amounts to EUR 16,000,000.00.

Further, 11 natural and two legal persons (applicants) were charged with an offence of trading in influence pursuant to Article 336 (2) of the Criminal Code.

Within individual interventions, financial resources amounting to EUR 537,800.00 (during the investigation, one accused person surrendered an additional amount of 400,000.00 which resulted from the above corruption criminal activity) and valuables (pictures, coins, collector postage stamps) in a total amount of EUR 2,214,000.00 were seized.

In this criminal offence, proceeds generated in the territory of the SR prevail; they are legalised in particular by handing over a commission to the person, who participated in subsidy allocation, through a fictitious transfer to third persons, by encumbering the property with third persons' rights (fictitious receivables), as well as by purchasing real estate, and to a negligible extent by investing on the capital market, etc.

In the monitored period, a part of allocated subsidies from EU funds and state budget was also abused by organised groups. Modus operandi of subsidy abuse was most frequently connected with the overestimation of projects co-funded from subsidies, after an agreement with the related persons holding decision-making/approving powers and acting in the competent management bodies of subsidy schemes. At the same time, after an agreement with the participating related persons, there was contrivance in tenders for the selection of project contractors in favour of winners selected in advance. Subsequently, these winners as project contractors invoiced fictitious or overpriced supplies of goods and services to investors/submitters of projects, who had them reimbursed from subsidies. The contractors then distributed the illegal commissions (proceeds) under the contracts to the persons interested, including those holding decision-making/approving powers from the managing bodies of the respective subsidy schemes, e.g., in the form fictitious contracts for the supply of services (consulting) or in cash.

The systemic steps of the current Government in managing and drawing subsidies reduce the current as well as future ML threat connected with subsidy frauds. It will also significantly reduce the overall ML threat. This is very important because in 2014 – 2020, the SR will receive about EUR 20.3 bn. from EU funds for structural and investment projects, for payments to farmers and for pan-European programmes. A considerable part of them has not been drawn yet.

According to the Annual Report of the European Anti-Fraud Office (OLAF) for 2017, an amount of EUR 631 mil., which had been illegally obtained within EU fund frauds in the SR, was returned to the EU treasury in the previous year. Slovak authorities themselves detected most of the irregularities in drawing European funds in Member States (at the same time, the SR had to return 2.55 % of paid EU funds based on OLAF investigations). Thus, in particular the way of subsidy drawing is a problem in the SR.

Out of the total number of criminal offences of economic nature, 166 cases are cases of damaging the European Communities' financial interests, which is only 0.34 % of criminal offences of economic nature. Out of the above number, there were 62 cases of conviction (a share of 37.35 %), and property in a total amount of EUR 532,802.00 was seized. One penalty of forfeiture of property was imposed for the monitored period.

The total damage caused by the criminal offence of damaging the European Communities' financial interests amounted to EUR 16,012,000.00, which is 0.79 % of all criminal offences of economic nature. There has been a gradual decrease over the years.

Compared to the previous assessment period, **there was a decrease in the number of detected cases by 107 cases and in the damage caused by EUR 276,273,000.00**. The reduced number of detected cases can be assigned to tightened rules in the area of withdrawal of financial resources from EU funds.

Explicitly it can be stated that the methods of commission of criminal offence of damaging the European Communities' financial interests in conjunction with subsidy frauds or contrivance in public procurement and public auction are under development every year. Perpetrators endeavour to ensure that the project documentation administratively meets the contractual or legal conditions for the provision of a financial contribution. Within the cases under investigation in 2016 to 2019 in connection with the offence of damaging the European Communities' financial interests it was not proved that workers making decision on the allocation of non-repayable financial contributions (hereinafter the "NFC") for individual providers had been involved in any way in the criminal activities[21].

Within the assessed period, on 1 July 2016, Act No. 91/2016 Coll. on criminal liability of legal persons came into effect; after implementation, it was reflected by **prosecution of legal persons for the criminal offence of damaging the European Communities' financial interests. Four legal persons were charged for the monitored period.**

In 2016, an investigation into the criminal offence of damaging the European Communities' financial interests pursuant to Article 261 of the Criminal Code in conjunction with a subsidy fraud pursuant to Article 225 of the Criminal Code at a stage of attempt pursuant to Article 14 (1) of the Criminal Code took place. The accused person in the position of a statutory representative of a legal person as the beneficiary and the Ministry of Economy of the Slovak Republic represented by the Slovak Innovation and Energy Agency (hereinafter the "SIEA") as the provider entered into a Contract of Provision of Non-Repayable Financial Contribution, whose subject matter was to provide a non-repayable financial contribution to implement the project "Research and development of complex access control systems". In mail delivered to the SIEA, the person submitted to the provider a forged document – "Binding Loan Commitment" of a bank on the approval of a loan for this legal person amounting to EUR

[21] However, in 2020, the former Director of the Agricultural Paying Agency (PPA) and a financier from the Slavia Capital Group were charged with a continuing particularly serious crime of receiving a bribe committed with accomplices in connection with the allocation of subsidies by the PPA. The bribes allegedly amounted to almost EUR one million.

1,050,000.00 for the purposes of co-financing of the project, which, however, had not been really issued by the bank. In another mail delivered to the SIEA, the person submitted to the provider mendacious take-over protocols on the take-over of calls for proposals of two companies, as well as a false price quotation of another company thus misleading the employees of the SIEA as regards the fulfilment of conditions for the provision of the NFC. By acting so, after submitting the application for NFC provision, the accused person attempted to elicit a contribution amounting to EUR 1,946,000.00 divided into EUR 1,654,100.00 (85 %) from the funds of the European Union, and EUR 291,900.00 (15 %) from the funds of the state budget of the Slovak Republic.

In documenting the predicate criminal offence of damaging the European Communities' financial interests for the assessment period 2016 – 2019, criminal prosecution for the **criminal offence of legalisation of proceeds of crime** took place in two cases with the names "PPA-controller" and "MPSVaR".

In the case of "PPA-controller", one of the perpetrators of the predicate criminal offence, after receiving from a mediator a bribe amounting to EUR 3,000.00 to their bank account for ensuring the approval of a Single Application for 2016 by the Agricultural Paying Agency, they withdrew the funds by means of a payment card in cash, thus legalising them.

In the case of "MPSVaR", after eliciting fraudulently a non-repayable financial contribution amounting to EUR 593,050.38, the perpetrator trying to conceal the origin of cash from criminal activities deposited the money into bank accounts in the Slovak Republic, from where the amount of EUR 424,319.00 was transferred to an account kept by a bank in the United States and used for the purchase of real estate in the USA, State of Florida.

2.4.4. Tax evasions as a source of illicit proceeds of organised crime

2.4.4.1. VAT frauds

Smuggling of goods, illicit production and sale of high-tax goods, frauds with excess value added tax (VAT) deductions have been main sources of proceeds of organised crime in the SR for a long time.

As in the previous assessment period, in the period 2016 to 2019 too, **carousel frauds** cause the biggest damage to the state budget; they are committed in trading in various commodities, as well as services with the objective to draw ineligible excess VAT deductions. This area is discussed in more detail in Chapter 2.4.2 Tax criminal offences – Tax Cobra.

2.4.4.2. Cigarette smuggling

Based on information obtained in the assessment period between 2016 and 2019 we can state that as in the previous period, **cigarette smuggling to Slovakia and further to the EU in particular through the border between Slovakia and Ukraine by Slovak-Ukrainian smuggling groups, often in cooperation with customs officers and policemen on both sides of the border, continues to prevail. Cigarettes are also illegally imported from Ukraine to the SR through Hungary or Poland.** In the assessed period, untaxed tobacco products with a

false identification of manufacturer were **also manufactured in the territory of the SR,** with the use of illegally imported tobacco.

In 2017, Slovak customs officers in Komárno seized over 2 tons of tobacco, from which 2.3 mil. cigarettes could have been manufactured. The tax evasion would have amounted to EUR 170,000.00.

Smuggled or illegally manufactured untaxed tobacco products were **distributed in the territory of the SR or further transported to those EU States (Austria, Germany, Italy)**, in which tobacco products are burdened with a higher excise tax.

According to a study of the advisory company KPMG,[22] **the consumption of illegally imported cigarettes continues to grow** in Slovakia. In 2016, the consumption of smuggled cigarettes represented a volume of 240 mil. pieces, in 2017 about 360 mil. pieces of cigarettes (an increase by 50%). The share of illegal cigarettes in the total consumption in 2017 amounted to 4.8%. In 2018, illegal cigarettes represented as much as 6 % of total consumption in Slovakia. If these cigarettes had been sold legally, the additionally obtained tax income would have reached EUR 44 mil.

Cigarettes are a naturally attractive article for illicit trade. In western Europe, a pack of branded cigarettes costs up to seven Euros, the price on the black market in western countries is about three Euros; the cost of production is counted in cents. In Slovakia, smuggled cigarettes are sold at half-price, sometimes at an even lower price than legal ones. In the whole EU, tax evasion amounts to EUR 10 bn. per year.

Traditional methods of transportation of contraband include concealments in cars, fuel tanks and goods wagons. Water way is also offered – inflatable boats without crew or drums on the Tisza River, or traditional crossing of the green border. Beneath the eastern border, customs officers also found a 700-metres-long tunnel equipped with rails and carts for the transportation of contraband. It was used two to three times a week, which corresponds to tax evasion of 50 mil. per year. The health warning messages on the packs of confiscated cigarettes were in English, thus they were probably not intended for the Slovak market. The use of drones – small unpiloted aircrafts flying over the border with contraband – is among the new trends recorded in the border area of Slovakia.

Perpetrators used the profit/proceeds illegally obtained from tax frauds in the monitored period for investments in purchases of real estate and precious metals, which also served as an underlying commodity in committing VAT frauds. Proceeds generated in the territory of the SR from criminal activities committed abroad prevail. According to the findings of Europol, in a broader sense, illicit trade in tobacco also represents a security threat.

Tobacco gets to illegal factories manufacturing cigarettes mostly from the Balkans, the other components necessary for the technological process of production of cigarettes (e.g.,

[22] Pursuant to the study of KPMG: "Study of the illicit cigarette market in the European Union, Norway and Switzerland" from 2017.

packs, cigarette paper, filters, etc.) are also imported from abroad, where these activities are legalised through foreign business companies, often with non-existent or hardly searchable persons interested with foreign bank accounts.

In this type of criminal activities, perpetrators naturally use cash to a maximum possible extent and for that reason, the seizure of any financial resources on bank accounts is considerably hindered, in many cases even impossible. In these cases, the cash found during searches of homes or searches of other premises or lands is seized.

The situation with the seizure of financial resources on accounts or draining of proceeds of crime is to a certain extent also complicated by the fact that criminal activities related to illicit manufacturing of cigarettes are more or less a privilege of foreign nationals (this concerns both the organisers and the workers working directly at these illegal production lines).

2.4.4.3. Frauds with alcohol and mineral oils

An increased risk of alcohol excise tax evasion consists in the fact that alcohol and liquor can be easily produced from freely available raw materials (fruit and other food commodities) and they can be relatively simply stored and distributed because of interchangeability with other goods. The illicit import (smuggling) of alcohol and liquors is less significant than cigarette smuggling.

Based on the knowledge of the tax and customs administration, as in the previous period, the methods of alcohol tax evasion include in particular the illicit manufacturing of alcohol (including by properly registered entities), illicit distillation of alcohol in home conditions, sale of illegally produced and imported liquors (in particular in pubs), sale of alcohol and liquors without licences, illicit import and export of alcohol and incorrect declaration of goods (cleaning agents, anti-icing agents, surfactants).

The alcohol for further use (dilution, flavouring, filling) is mostly imported from Poland due to more liberal laws concerning alcohol and liquor management than in the Slovak Republic.

In the area of mineral oil excise tax evasion, the internationally operating groups use the modus operandi of declaration of goods different from the goods really sold. For example, when being imported, diesel oil is declared as mineral heating oil or lubrication oil, whose excise taxes are much lower because they are intended for other purposes than fuels. Subsequently, diesel oil is sold to retail consumers through a network of Slovak, as well as foreign companies without lodging excise tax and VAT returns and without paying these taxes. During the commission of the criminal activities, the companies are changing. The places of declared unloading of the oil are also changed, mostly in other Member States.

With respect to the absence of accompanying documents to this mineral oil, there is a problem with the documenting of its movement in real time and subsequently proving its offer or use as fuel (which is the fact establishing the tax liability).

Perpetrators used the profit/proceeds obtained illegally from tax frauds in the monitored period for personal consumption. Proceeds generated in the SR, i.e., domestic proceeds consumed in the SR, prevail.

In 2018, during an action, the joint investigation team of the Slovak Financial Administration Criminal Office (FACO), Czech Police and customs officers from the Customs Office for the South Moravian Region seized 11,000 litres of illegal mineral oil. The action was focused on the dismantling of an international organised group trading mineral oils transported from Poland to other EU Member States through the territory of the Czech Republic and Slovak Republic. Mineral oils were purchased in Poland, then unloaded at various places in Slovakia and sold to customers as fuel – diesel oil. They also should have been transported to Austria; however, they were sold illegally in Slovakia without tax payment. During the action, eight persons were detained and charged by the investigator of the Financial Administration with the criminal offence of Tax and insurance premium evasion, Article 276 of the Criminal Code. The excise tax loss quantified preliminarily amounted to EUR 500,000.00 and VAT loss at least EUR 200,000.00.

2.4.4.4. Tax and customs duty evasion in illegal import of goods, Asian OCG.

Groups of Asian organised crime (mostly Chinese and Vietnamese) are relatively **well established** in particular in the neighbouring States (Czech Republic, Poland, Hungary), but with business and personnel connections in Slovakia. They commit in particular criminal offences of economic nature, preferably they import goods with a fraudulently low customs value (forged invoices), smuggle goods, evade taxes in selling goods, counterfeit branded goods. The entities controlled by persons from Asia illegally import Asian goods through front companies. These persons also provide for the contacts to customs administration, preparation of fraudulent customs declarations covering the goods, accounting, lending and exchange of money. In 2017, goods for over EUR 5 bn. were imported from China to Slovakia according to the Statistical Office. Electronic goods represented the biggest share.

Most frequently, the perpetrators (Asian exporters) declare a lower price or quantity of imported goods (decreased by 60-90%) with the objective to pay lower import duties, and submit forged documents of goods origin with the objective to avoid quotas or import or antidumping duties. Customs officers have limited possibilities of verifying the authenticity of invoices and value of goods, for which duties are paid – in particular for the goods from China.

In most cases, the subject of such illicit trade is import of textile products, footwear and consumer goods. According to customs analysts, customs and tax debts also occur because the imported goods do not end in our territory and continue to the neighbouring countries. The trend of transportation of counterfeited goods from the surrounding EU countries, in particular from Poland and Hungary, also continues.

In contrast to previous years, the situation has changed mainly due to the amended legislation. The goods infringing the intellectual property rights greatly disappear from shops and markets. The establishment of the Interministerial Commission for the Coordination of Cooperation to Combat Counterfeiting and Piracy under the competence of the Industrial Property Office of the SR also contributed to situation improvement.

Today, the sale of goods via the internet is increasingly emerging; it attacks the intellectual property rights in a similar way. Risky goods in this area include in particular perfumes, electronic goods and medicines.

The profit/proceeds from such illegal activity are either invested in real estate in the SR or transferred outside the EU to South-East Asia by couriers beyond the border and then by bank transfers from an EU Member State or non-EU State. Groups also legalise proceeds in the form of partially fictitious foreign-trade operations (overestimation of revenues). The scheme may also include cash deposits of high amounts into bank accounts of companies. Their Executive Officers are from the Asian community or straw men and the rights of disposal of their bank accounts are held by Asian people. Proceeds generated in the territory of the SR from criminal activities committed both abroad and in the SR prevail.

2.4.4.5. Threats resulting from the abuse of Slovak business companies

The overall ML threat of abuse of forms and schemes of business companies is high, there is a significant disproportion between the revealed and latent criminal activity. Without the performance of proactive financial investigation, the volume of generated proceeds identified is substantially lower than the one really generated.

As in the previous assessment period, in 2016 to 2019, it can also be stated that the involvement of Slovak business companies in the criminal activities generating proceeds in serious cross-border criminality is manifested in particular in criminal offences of economic nature.

In this connection, the SR can be characterised as:

- **a target country** – straw men are installed in the positions of statutory representatives of companies, who are managed by another person (perpetrator) standing outside the company and issuing orders, in particular for withdrawal of financial resources from the company's accounts that were obtained by various fraudulent activities (tax frauds, credit frauds),
- **a transit country**, where Slovak companies are used to transfer financial resources abroad, in particular to China (Baltic countries - China, Romania - China).

A significant group of criminal offences involving business companies is represented by **carousel frauds** (fictitious circulation of goods, emission allowances), which involve two to three States at regional level (CR-SR, CR-SR-HU, PL-SR-HU). This area is discussed in more detail above, in Chapter 2.4.4.1. "VAT frauds".

CEO frauds represent a significant degree of ML threat with a slightly increased tendency in terms of the way of committing criminal activities and the proportion of undetected volume of proceeds generated.

The so-called **CEO frauds**[23)] include a targeted attack based on social engineering with the objective to mislead an employee so that they transfer certain amounts of money abroad. Thus, CEO fraud is essentially a fraud with payment order, it is characterised by sophisticated, harmonised and self-serving attack in particular against private persons and companies, and in general, it is organised by one managing group. The essential attribute is activity, which also moves this type of criminal activity to the **sphere of cybercrimes**. It is necessary to crack the securing of the CEO manager's e-mail communication provided that their mailbox contains information on the business activities under way and on the e-mail addresses of individual employees.

Finding the perpetrator of such criminal activity is difficult because the perpetrator mostly communicates from abroad and prevailingly in electronic form. In the cases when criminal proceedings are under way, the results of investigation depend on the results of international legal assistance. **The main causes of the failure to clear up these cases definitely include the international aspect and modern ways of concealing the perpetrator's identity through electronic communication**.

However, in the monitored period, "failures" of perpetrators were also recorded due to the caution of the affected CEO managers or due to security measures in the form of additional verification or double approval of transfers of the company's money, thus, the completion of criminal offence was prevented.

As in the previous assessment period, in the SR, the most frequent type of CEO fraud is a false e-mail followed by a fraud through a modified invoice.

Based on available information it is possible state that in the previous assessment period, the detected CEO frauds showed a stagnating tendency (up to 20 cases per year). Within the comparison of the years 2016 to 2019, in 2017, a rising trend was recorded (45 cases) to more than double compared to the previous years, and in 2018, a downward trend was again recorded (27 cases). In the long term, a stagnating or downward tendency of recorded CEO frauds can be seen. More attempts than completed acts were recorded.

The damage caused by CEO frauds reaches high amounts; in 2018, the damage amounted to over EUR 405,000.00. Compared to the previous year, the damage found was higher for both the completed cases and for cases at a stage of attempt. Of course, the total amount of damage is affected in particular by the number of cases. For the above reason, the evaluation of the rate of damage (i.e., the average damage amount in one case) is suitable for the purpose or more objective assessment.

The recorded cases of **CEO frauds are qualified as a criminal offence of fraud pursuant to Article 221 of the Criminal Code**. For better statistical monitoring of CEO frauds compared to "traditional" frauds, code 858 – "Fraud in connection with false transfer of money based on an instruction from a fictitious manager" was added to the code-list of the Crime Recording and Statistical System (hereinafter the "ESSK") on 1 October 2017.

[23)] Analysis of the criminal activity of CEO frauds in the SR – prepared by the Police Criminal Office of the PPF

Within the characteristics of CEO frauds, a concurrence of criminal offences of fraud pursuant to Article 221 of the Criminal Code and cybercrime pursuant to Article 247 et seq. of the Criminal Code can occur.

As regards individual cases of CEO frauds, it should be noted with respect to the following activity of perpetrators that it is also a predicate criminal offence for the subsequent legalisation of proceeds obtained by them from crime. Thus, in the SR, CEO frauds can be followed by another criminal offence of legalisation of proceeds of crime pursuant to Article 233 of the Criminal Code, and in justified cases, also a criminal offence of sharing pursuant to Article 231 of the Criminal Code and 232 of the Criminal Code. It is the criminal offence of legalisation of proceeds of crime, which connects the cases showing signs of a CEO fraud because the method used by the perpetrator to transfer the obtained financial resources and withdraw them is also the greatest weakness in the complicated structure of CEO fraud. The time from eliciting the financial resources to their gradual transfer to the perpetrator's account or to other accounts (legalisation) plays an important role in these cases.

The SR belongs to a group of countries (SR, CR, Hungary, Poland), through which the transit of the financial resources from such cases committed abroad is carried out. This state results from legislative gaps in particular in the area of financial market utilised by perpetrators during the transfers of financial resources executed among EU States. Purposive opening of accounts for the commission of CEO frauds became a lucrative source of income in the SR in particular for foreigners.

In this connection it should be noted that in addition to the cases of CEO frauds detected by the Criminal Police Office, the cases of CEO frauds, in which financial resources **were elicited abroad from a foreign company and remitted to accounts kept in the SR,** were also solved in the territory of the SR. **These cases were detected on the basis of unusual transaction notification by the FIU SR of the PPF, and for the reason of the need to seize the financial resources on the account, criminal proceedings were commenced for a criminal offence of fraud pursuant to Article 221 of the Criminal Code.**

In 2017, the FIU SR received a report concerning a foreign payment amounting to about EUR 1,400,000.00, which was fraudulently transferred from a foreign account kept in Chile and belonging to a company based there to an account in the SR kept for a Czech business company. After the funds had been credited to the account of the Czech company, two cashless urgent payments in the amounts of EUR 150,000.00 and EUR 20,000.00 were immediately made from the account abroad – to two accounts kept by a bank in Poland. At the same time, the Slovak bank received from the foreign correspondence bank the first SWIFT message with a request for return of the payment made from Chile in the amount of about EUR 1,400,000.00 to the account of the Czech company, in which the foreign bank from Chile stated that the Chilean company had become victim of the so-called CEO fraud. Subsequently, the Slovak bank took technical measures on the account of the Czech company for potential suspension of unusual transaction in accordance with Article 16 of the AML Act in order to prevent any further disposal of the balance on the account. The FIU SR immediately informed the partner FIU Poland on the above two payments from CEO fraud in the amount of EUR 170,000.00 made to two Polish accounts. Immediately after this information had been sent, both payments were returned from the accounts from Poland back to the account of the Czech company in the

SR. Subsequently, the FIU SR prepared and forwarded comprehensive information to law enforcement authorities. Based on the forwarded information, a criminal prosecution for a suspicion of commission of a criminal offence of legalisation of proceeds of crime was commenced, and then the competent Prosecutor's Office seized financial resources amounting to approximately EUR 1,400,000.00 on the account of the Czech company.

2.4.5. Other ML aspects resulting from the typology of abuse of legal persons

2.4.5.1. ML threat factors

From the view of individual factors, legal persons operating in the sector of banking, trade and services, intermediary and advisory services seem to be the biggest threat for ML. Limited liability companies and joint-stock companies are the riskiest form of legal persons used for ML.

In the previous assessment period, 299,464 business companies operated in the territory of the SR,[24] and about 1000 new business companies are established every day[25]. Today, 72,440 legal persons[26] (interest associations, associations of flat owners, political parties and movements, organisations with an international element, civic associations, trade unions, associations with confirmed activity, trade communities, non-profit organisations and non-investment funds) are registered in registers and records of the Ministry of Interior of the SR, of which 50,000 are civic associations.

Based on information found during the assessment period and below mentioned factors, the following types of legal persons were identified as representing **the biggest threat for ML cases**:

By sectors:

- banks,
- legal persons running a business in trade and services (in particular mediatory and advisory activities).

[24] Enterprise statistics/economic entities according to selected indicators, available on 25 October 2017, at: https://slovak.statistics.sk/wps/portal/ext/themes/special/economic/!ut/p/z1/pZNNb4QgEIZ_EiOC6BGxslTjB6665dJ42pi02x6a_v5idxOTkoU25UbmfWaYlxlk0AmZy_K5npeP9e2yvNj7k0mee6bSPI84pPmEQbFGR1XfS1wwNP8QNPoB1JF3Uj-SCAhFxobLocM8I1IUui1tWOB0qBMMEN14j8Dcr19F5MYLyQ-E1QBpLSkofhh11scx8NjH7--HO4fD7_hdQBmAaoYRYBpgAPD2L5NA_1bwx_qOQR5eZTjAj-xf_CbY-KnuruF2GLm1Rysq6jxuBXH4SggroMeCTk3cOf479l55TwHjTz-HBtz4x2NG5lvim8BQDhNaEuPdgu2TQmNmfP-QltQp4Rj1_jru5wSrWtX5C6wX0H4!/dz/d5/L2dJQSEvUUt3QS80TmxFL1o2X1ZMUDhCQjFBMEc3VDEwSU5OU1VWOFEzUTg1/.
[25] Ibid.
[26] interest associations, associations of flat owners, political parties and movements, organisations with an international element, civic associations, trade unions, associations with confirmed activity, trade communities, non-profit organisations and non-investment funds. Individual registers available on 25 October 2017 at https://www.minv.sk/?registre-evidencie-zoznamy-informacie-o-registracii.

By types and legal form:

- limited liability company,
- joint-stock company.

2.4.5.2. Sector ML typology of legal persons

2.4.5.2.1. Banks

Legalisation and coverage by legitimately operating enterprises generating cash on a regular basis is among the most frequent methods used to introduce illegally obtained financial resources into the financial system. Within the banking system, electronic transfers are used to transfer financial resources and to a considerable extent, they are used to conceal the legalisation of proceeds of crime utilising their features such as speed, security and low costs.

As regards the structure of products, in particular payment accounts for legal persons – small or medium enterprises (so-called SME customers[27]), which are the riskiest ones, are concerned. **Legalisation and coverage by legitimately operating small and medium enterprises (in particular limited liability companies) generating cash on a regular basis is among the most frequent methods used to introduce illegally obtained financial resources into the financial system.** The fact that cash deposits volumes are about 1.5-times bigger than cash withdrawals is a negative phenomenon of this product. The total volume of cash deposits into payments accounts of enterprises at all banks amounts to approximately EUR 16 bn. (which means about 21% of GDP for 2015).

2.4.5.2.2. Legal persons running a business in trade and services

The use of enterprises creating income consists in mixing the illicit financial resources with the financial flow from seemingly lawful business. The examples of enterprises generating high income include consulting, advisory and management companies, pubs, restaurants, car wash services, etc., as well as **every legal person, which has or can have low costs as a consequence of a small number of necessary suppliers, and which creates cash profits or whose product's value can be examined and determined only with difficulties** (consulting and advisory services including accounting, tax and legal services, marketing analyses, etc.).

The high rate of risk of this segment is confirmed and interconnected with the above banking products because the overwhelming majority of entities using bank payment accounts in the segment of SME, which represent the riskiest banking product in terms of ML, are business limited liability companies.

Moreover, if control is carried out, it is highly improbable that complete and real volume of really performed activity will be found. The ML risk in this segment also consists in the fact that certain key activities for ML are carried out by entities bound by confidentiality and have ex lege exception from UT reporting, including the risk that most entities running a business in trade and services are not obliged entities according to the ML legislation.

[27] Small and Medium Enterprise

2.4.5.3. Typology of legal persons

2.4.5.3.1. Limited liability company

As regards the rate of ML risk of individual types of legal persons, in particular limited liability companies as the most frequent legal form of a business legal person in the SR need to be included here. This trend is also confirmed by huge fluctuation of establishment of new business companies, which often do not carry out any activity; they are exclusively SPV (Special Purpose Vehicles) for tax accounting purposes. At the same time, this legal form is also mostly used in individual sectors, and also uses the riskiest banking product from the view of ML, i.e., a payment account for the SME segment.

2.4.5.3.2. Joint-stock company

As regards the rate of ML risk of individual types of legal persons, joint-stock companies should also be included here because all banks and insurance companies are ex lege obliged to carry out their activity as joint-stock companies. It also applies to this form of business company that its ownership structure cannot be verified immediately, just by looking into the Commercial Register; a request is necessary to the Central Securities Depository. This means a higher rate of anonymity of shareholders. However, the ML risk of banks is reduced by regulatory standards of the National Bank of Slovakia, which also oversees and supervises, inter alia, the ownership structure of banks.

2.4.6. Forecast of ML threat development in criminal offences of economic nature

Criminal offences of economic nature will have a rising tendency. The increasing patronage, corruption, poor social situation, free movement of people and goods, poor law enforcement and pursuit of wealth are considered the most important acceleration factors of the future development.

Improvement of control by supervisory authorities, legislation changes, in particular stricter penalties, improvement of work of law enforcement authorities are considered the most significant factors of weakening.

In particular tax criminal activities will continue to have the highest potential of generating proceeds of criminal offences of economic nature; it is expected that these criminal activities will be committed mostly in an organised manner and with a high rate of utilisation of sophisticated schemes of legal persons, with a cross-border aspect within the EU and outside the EU (a high latency possible).

The number of cases of CEO frauds, phishing, etc., is expected to have a decreasing tendency. However, a significant increase can be expected in internet frauds, due to an increase in the interest of the population in purchasing goods online, which is also supported by the current situation of COVID-19 spread all around the world.

The acceleration factor of the threat of generating high profits from tax criminal activities will be supported by the fact that the damage caused by this type of criminal activity is high, and by the high tolerance of the public in relation to tax criminal activities, where based on survey, as many as 89 % of respondents[28] tolerate this type of criminal activity.

The elements, which can negatively affect the above type of crime (in particular frauds), include the constantly improving possibility and usability of cyberspace (abuse of online space) and the related speed, cross-border character, and a considerable rate of anonymity during individual (fraudulent) activities.

2.5. Corruption crimes[29]

2.5.1. ML threat factors

As regards the threat of generating proceeds of crime, corruption represents a medium-high level of ML threat, without substantial trend fluctuation, in particular with reference to the fact that the assumed amount of unrecorded proceeds is with respect to their character definitely higher compared to the proceeds identified within the really prosecuted corruption criminal activities.

According to the evaluation of the SR within the CORRUPTION PERCEPTIONS INDEX **issued on an annual basis by Transparency International,**[30] since 2017, Slovakia has been reaching only 50 points out of 100 points possible (in 2016 only 51 points, in 2020 – 49). Out of EU countries, only five countries have a lower score – Hungary, Greece, Croatia, Romania and Bulgaria.

The unsuccessful fight against serious cases of corruption in the second half of the decade is also confirmed by a survey carried out by Transparency International at the end of 2019 on the basis of verdicts of the Special Criminal Court. Two thirds of penalised cases concern small corruption up to EUR 500.00, 40 % even up to EUR 100.00. Moreover, the total number of concluded cases in 2016 – 2019 dropped by one third compared to 2011 - 2015. The number of convicted politicians, judges, policemen or prosecutors also dropped considerably. In the current electoral term till October 2019, there were only 12 such cases, whereas there were 30 of them in the previous one. However, this state concerning **corruption in justice also substantially changed in 2019 and 2020;** charges were brought in several cases of corruption of judges at the level of District and Regional Courts falling under the competence of the Regional Courts Bratislava and Žilina.

In the cases including high bribes, investigation procedure is usually proactive, thus, the perpetrators were detained immediately after receiving a bribe; therefore, they could not launder the funds and obtain benefit for themselves.

[28] Source of survey: Academy of the PF

[29] Abuse of power by a public official Article 326 (old Article 158), Receiving a bribe Articles 328, 329, 330 (old Articles 160, 160a, 160b), Bribery Articles 332, 333, 334 (old Articles 161, 161a, 161b), Trading in influence Article 336 (old Article 162), Electoral corruption Article 336a, Corruption in sport Article 336b

[30] https://www.transparency.org/en/cpi/2019/index/svk

In corruption crimes, **domestic proceeds generated in the territory of the SR are concerned**. The proceeds are most frequently used for the payment of reward for arranging the provision of service, purchase of real estate, fictitious transfers to third persons, burdening the property by third persons' rights (fictitious receivables), etc.

As a consequence of globalisation, free movement of goods and services, influence of international financial groups, the economy of the SR's size **is not protected against these practices and all related threats, either.** Thus, the SR is still attractive for foreign direct investments (FDI) because of simplicity of establishment of a business company in Slovakia and low costs of trained labour.

The SR **as part of the EU** depends on the efficiency of instruments adopted at EU level in the area of eliminating of conditions for the abuse of the European mechanism for money laundering. In this context, however, the fulfilment of implementation and transformation duties resulting from the membership in the EU is a significant challenge. These duties are not fulfilled sufficiently actively. The examples include a delay in the transposition of both AMLD 4 and 5, or particular significant deficits in the area of building and the threat to subsequent integration of the register of beneficial owners, and the current transposition deficit in building a central register of accounts (and likewise, the threat to its integration into the EU mechanism).

Important procedural methods for revealing and taking of evidence of corruption include in particular the use of an agent, tracing people and things (operational and search activity means), interception and recording of telecommunication operation, preparation of video and audio recording (information technical means), checking the bank accounts, seizure and analysis of computer data. Taking into account that these methods usually infringe the constitutional rights of citizens, their use requires high expertise of policemen, prosecutors and judges.

A principle applies to corruption that the success of the fight against this phenomenon is increased if it is detected and evidenced in real time, at the time of commission of the criminal activity (online). Corruption detection and taking of evidence ex post is usually unsuccessful in particular due to the extinction or unachievability of relevant evidence.

The success rate of corruption detection and taking of evidence is, however, determined by timely application of the above procedural methods. The primary source of information on corruption perpetrators for law enforcement authorities are whistle blowers, their own operational search activities or intelligence information (SIS, MI).

Compared to the previous assessment period, there was a significant decrease **in corruption crimes** by 764 cases, when 774 cases in total were detected in the monitored period 2016 to 2019 representing 0.30 % of overall criminality. **A downward trend is seen** over years.

The number of corruption crimes decreases, inter alia, because the persons asked for bribe strongly refuse to hand over a bribe during an initial meeting. Another reason for the decrease was a low activity of the anti-corruption police in the period 2016-2019, which, however, started significantly changing from 2019. Although the established anti-corruption telephone lines caused expanded reporting, it only brought general suspicions of things that had already happened or without any detailed circumstances.

After an analysis of the cases executed in the assessed period it can be stated that compared to the previous assessment, corruption activities move to a qualitatively higher and more sophisticated level.

Based on the analysis of cases for the period 2016 to 2019, it can be noted in relation to the entities charged with corruption crimes that they included persons from general government (e.g., civil servants, employees of municipality offices, members of municipal councils, etc.) and services (e.g., controller of urban mass transportation, doctors, referees), as well as corruption activities in the judicial system, prosecutor's office, in the area of approval and withdrawal of non-repayable financial contributions from EU funds, in awarding and executing contracts within companies with the majority participation of the State, in awarding and executing contracts within private companies in drawing non-repayable financial contributions, in performing local government, in healthcare and education.

2.5.1.1. Method of asking for and offering bribes

In detecting and investigating corruption crimes, the following ways of conduct of perpetrators prevailed:

- they do not express the request and offer directly but without a bribe, they knowingly handle the matter of individual or public interest with delay and problems,
- they express the request for a bribe and offer of a bribe through an intermediary or even several persons,
- the request and offer are not expressed directly but it is known from "history" and friends that bribe is offered or received as a matter of course, in particular in the form of services and non-material benefits,
- direct request for a bribe either in the form of cash according to the contract size or a reciprocal service in the form of certain work performance by the company.

2.5.1.2. Place and form of bribe acceptance and hand-over

In the assessed period, the persons charged with corruption crimes handed over and accepted bribes mostly:

- in cash in an office or workplace of the bribe recipient,
- bribe acceptance and hand-over at public places (car park, restaurant, shopping centre, etc.), and
- bribe acceptance by crediting to a bank account covered by a fictitious service is a novelty compared to the previous assessment.

As regards the form of bribes, pecuniary bribes in the currently valid EUR currency prevailed.

Corruption mostly occurred in connection with the procurement of a thing of public interest. The areas such as healthcare, land register departments, district offices and tax authorities were concerned.

In the monitored period 2016 to 2019, corruption crimes were cleared up, in which the total **amount of requested bribes amounted to EUR 2,015,709.00 and the sum of really accepted bribes amounted to EUR 1,704,908.00**. In connection with corruption crimes, **a total amount of offered bribes of EUR 1,663,061.00 was documented, and the funds amounting to EUR 829,185.00 were really handed over**.

As regards related criminal offences with a potential of ML threat it should be noted that the most frequent criminal offence against public order was the criminal offence of abuse of power by a public official, for which 223 criminal prosecutions were started, 239 persons were indicted, 126 persons were convicted, and one penalty of forfeiture of a thing was imposed in the monitored period. For the monitored period, this crime caused a total damage amounting to EUR 10,412,000.00.

The criminal prosecutions commenced in 2019 and 2020 showed that other important criminal offences directly connected with the commission of legalisation of proceeds of crime include the **criminal offence of breach of trust by maladministration of estates of another pursuant to Article 237 of the Criminal Code and criminal offence of contrivance in public procurement and public auction pursuant to Article 266 of the Criminal Code**. The reason is that public procurements and State property administration include the handling and disposal of great amounts of money owned by the State and from State subsidies and the EU, which represents a high risk for corruption behaviour of persons holding decision-making powers in this area.

Taking into account the high amounts of financial resources included in public procurements and State property management, there is a high probability that bribes, often amounting to 10 and more percent of the contract value, will be in such amounts that legalisation schemes will be necessary to use and draw them.

In this context, it is extraordinarily difficult to estimate the scope of unreported criminality or the volume of sources coming from such activity.

In detecting and taking of evidence of corruption, investigation should also be focused on the financial review of the perpetrator by checking their bank accounts, seizure of movable and immovable property, analysing material data carriers and computer data. Shortcomings include the fact that no central register of bank accounts has been established, and ascertaining information, which is subject to bank secret, is time-consuming. It is not possible to monitor the movements on the account at the actual time of corruption commission, either. The Slovak Republic does not have a sufficient legal basis for such property monitoring, it is virtually only possible to retrospectively ascertain the state of the account or monitor the perpetrator’s real estate handling by screening and sending new and supplementary requests. However, in such case it does not mean active monitoring of property in real time, which allows the perpetrators of criminal offences, not only corruption, to successfully get rid of property with the objective to avoid the risk of property seizure, penalty of forfeiture of property or duty to reimburse the damage.

A low level of operational and in particular, analytical activities of the National Anti-Corruption Unit in the monitored period contributed to a low rate of detection and clear-up of serious corruption cases, where also legalisation of corruption proceeds can be expected.

Within its operational activities, the National Anti-Corruption Unit focused on and partially successfully detected in particular less serious cases of corruption at offices, stations of technical inspection of cars, police controls, outpatient departments, etc., when perpetrators receive bribes repeatedly, however, in relatively low amounts and in connection with handling their usual working matters. However, the operational and analytical activity of the police only marginally and with small efficiency focused on the detection of complicated corruption schemes in public procurements, allocation of subsidies from the budget of the Slovak Republic and European Union, high-value public contracts and similar serious matters, where huge wastage of public finances occurs. **One of the main reasons of low efficiency in detecting such corruption can be seen in the fact that the analytical component of the police still fails to a considerable extent. In particular at initial stages still before the commencement of criminal prosecution, it should perform analyses of financial flows or personal and property relations among suspicious persons in order to obtain a basic knowledge of whether a benefit from a particular suspicious operation could have been obtained by persons affecting the decision on a particular contract, subsidy or other handling of public resources**. The operational units encounter, inter alia, lack of professional staff, as well as legislative problems, when, for example, during operational detection of corruption, a policeman cannot request statements of accounts of the suspicious persons from banks in accordance with Article 29a (4) of Act No. 191/1993 Coll. on the Police Force as amended, despite the fact that the police are entitled to do so in some other criminal offences (tax evasions, illicit financial operations or legalisation of proceeds of crime). Moreover, in evaluating knowledge based on prosecutor's supervision in corruption criminal cases it was found out that even in 2019 but in particular in **previous years, the detection of complicated corruption cases encountered various artificially created limitations within the organisation of the police, in particular in the willingness and possibilities of conducting proactive financial investigation.**

As regards corruption reporting by other state authorities, in particular by other police units, SIS, National Security Authority, Supreme Audit Office or Financial Intelligence Unit, it is also necessary to note that only few relevant suggestions and information were received from them in the monitored period by the National Anti-Corruption Unit and led to detection of corruption criminal cases. Closer cooperation with these authorities could lead to much better efficiency in detecting and documenting corruption. In the previous months, some sign of improvement of this cooperation of some of the above units with the anti-corruption unit of NAKA was noticed, however, it will be necessary to adjust the whole system of cooperation so that each of the above authorities will take part in detecting possible corruption crimes under their competence and forward knowledge found to NAKA on a regular basis. The Financial Intelligence Unit of the PPF should play one of key roles in this context. Such cooperation across state authorities may lead to a considerable increase in the detection of corruption criminal cases.

If not in other areas but in the area of detection and criminal prosecution of corruption, a positive trend of prosecution of legalisation of proceeds of crime starting from 2019 should be pointed out.

Since 2019, despite the persisting of some system problems suggested above, a considerable improvement in the area of detection and prosecution of serious corruption crimes in several cases connected with legalisation of proceeds of crime has been recorded. This can be unambiguously documented by the following criminal cases executed in 2019 and 2020:

1. In 2019, criminal proceedings were conducted for the criminal offence of receiving a bribe pursuant to Article 328 of the Criminal Code, when the perpetrator, by extensive corruption criminal activities, "had arranged" judgements as desired by criminally prosecuted persons at courts in the district of the Regional Court in Žilina. The perpetrator was also charged with the criminal offence of legalisation of proceeds of crime pursuant to Article 233 of the Criminal Code. As they disposed of financial resources amounting to at least EUR 64,000.00 obtained from proceeds of corruption crimes, with which they were charged, and they were going to conceal the existence of such income in an undetected amount and thwart its seizure, forfeiture or confiscation for the purposes of criminal proceedings, the perpetrator consumed the assets, partially hid them and transferred to natural persons for disposal as interest-bearing loans provided as non-bank loans. In connection with the investigation of a predicate criminal offence (receiving a bribe), within the performance of procedural acts, an amount of EUR 226,000.00 was seized in a bank safe deposit box as proceeds of corruption crimes committed in the long term.

2. In 2019, a prosecutor indicted two natural and three legal persons for a continuing crime of receiving a bribe pursuant to Article 329 in concurrence with a continuing particularly serious crime of legalisation of proceeds of crime pursuant to Article 233 of the Criminal Code, which occurred so that at least since 2017, the persons designated as XX, Ing. XX, Ing. XX and Ing. XX had acted in cahoots, where Mgr. XX had ensured the appointment of Ing. XX as Head at the District Office in Bratislava, Department of Environmental Protection (hereinafter "OU BA OSŽP") as of 1 November 2016, as a person holding powers in proceedings conducted at OU BA OSŽP, with the intention to obtain unjust property benefit for themselves, as well as for natural persons Ing. XX, Ing. XX and Ing. XX, or for the legal persons managed by them, where XX also according to instructions of XX within their function had ensured through their subordinates the preparation of background documents and issuance of positive decisions and opinions, the signature of which by Ing. XX had been conditioned by providing bribes, whose amounts had been set on a case-by-case basis, according to the type of application, after the mutual agreement among Mgr. XX, Ing. XX and Ing. XX, and bribes had been requested from individual applicants through Ing. XX and Ing. XX, in particular in the form of mandate contracts entered into in accordance with the provisions of Article 566 et seq. of the Commercial Code, the subject matter of which had been the "Negotiation of application lodged with the District Office Bratislava, Department of Environmental Protection, for the purpose of obtaining a positive opinion or decision", and the decisions on dividing such received bribes had been made by XX; the contracts and the legal acts resulting from them or following them and several bank transactions through the companies managed by Ing. XX only had served to conceal the origin of the funds obtained by corruption activities.

3. Further, in 2020, several natural persons and legal persons were charged with a continuing criminal offence of receiving a bribe pursuant to Article 329 (1), (2) of the Criminal

Code committed in the form of abetting pursuant to Article 21 (1) (a) of the Criminal Code in concurrence with a continuing particularly serious crime of legalisation of proceeds of crime pursuant to Article 233 (1) (a), (3) (c), (4) (a) of the Criminal Code, which occurred in such a way that in the period from at least the beginning of 2017 to March 2020, in Bratislava and at other places in the territory of the Slovak Republic and in the territory of the Republic of Austria, the persons designated as Ing. JK, PhD., MK and Ing. M K PhD. had acted in cahoots for the purpose of committing corruption crimes, as well as legalisation of proceeds of crime, where Ing. J K, PhD., holding the position of the General Director of the Agricultural Paying Agency (PPA), as a person holding the power in proceedings conducted at the PPA, with the intention to obtain unjust property benefit for themselves, as well as for other natural persons or for legal persons managed by them and related by staff or shares, had ensured the issuance of positive decisions on the approval of non-repayable financial contributions conditioned by the provision of cash as a bribe amounting to 10% of the total amount of the requested NFC; the bribes had been requested from individual applicants through MVDr. Ľ K, in the form of a contract for work in accordance with Article 536 et seq. of the Commercial Code as amended, whose subject matter had been, inter alia, "Obtaining a positive decision on NFC approval"; the contracts and the legal acts resulting from them or following them and several bank transactions through the companies managed by them had only served to conceal the origin of the financial resources acquired by corruption activities. Some of the accused persons were detained for the above criminal activities.

4. Another case, when in 2020, a charge was brought for the criminal offence of receiving a bribe pursuant to Article 329 (1), (2) of the Criminal Code committed in the form of abetting pursuant to Article 21 (1) (a) of the Criminal Code in concurrence with a continuing particularly serious crime of legalisation of proceeds of crime pursuant to Article 233 (1) (a), (3) (c), (4) (a) of the Criminal Code, is the case of the Chairman of the Administration of State Material Reserves of the Slovak Republic (ASMR) who had allegedly committed corruption and legalisation activities in such a way that until 2020, as the Chairman of the ASMR, along with Ing. JJ as the General Director of the State Material Reserves Section of the ASMR, as the Director of the Department of Mobilization Reserves and Emergency Stocks acting on behalf of the ASMR, within the exercise of their authorisations resulting from their functions concerning the selection of particular suppliers and establishment of business legal relationships or conclusion of contracts under the competence of the ASMR, they had repeatedly, by acting in conflict with Article 10 (2), (3) and Article 42 (1) (b) of Act No. 343/2015 Coll. on public procurement, purposively influenced the announcement and course of public procurements of the ASMR as the Contracting Authority in such a way that they had manipulated market surveys for the purpose of determination of the expected contract value for a promised property benefit from future suppliers, they had purposively modified tender documents so that they had been suitable for a particular future supplier and in order to restrict the possibility of sending a bid by other tenderers, or they had manipulated the course of bid evaluation in order to ensure the winning in public procurements and subsequent property benefit of the business company M, for which they had subsequently received property benefit from the winning business companies in the form of payments and in kind rewards, which were concealed as payments of rent for leased real estate and subsequently a fictitious purchase of two flats in favour of KK worth EUR 200,000.00, for which he had not intended to pay. In this case, too, the accused persons were prosecuted in custody.

5. Another criminal case, when in 2020, a charge was brought for the offence of bribery pursuant to Article 333 (1) (2) (b) of the Criminal Code in concurrence with the criminal offence of legalisation of proceeds of crime pursuant to Article 233, is the following criminal case: At a meeting, accused PC along with accused MS offered a bribe to Ing. M F currently holding the position of the 1st State Secretary of the Ministry of Agriculture and Rural Development of the Slovak Republic, in the form of provision of 5% of the value of the bid which they had submitted in public procurement within a project with the title "Central data repository of the Central Control and Testing Institute in Agriculture – a comprehensive project for data management" worth EUR 1,497,614.40, for which IMF holding the position of State Secretary would ensure the continuation of public procurement, announcement of the winner of public procurement – their company, and subsequently, he would sign a contract of implementation of the project; the payment of the above bribe amounting to 5% of the value of the bid submitted in the above public procurement was to be made so that Ing. MF would provide a business company, which would provide unspecified services within a subsupply, these services would be accepted by the accused persons where in fact, the company Lomtec.com a.s. did not need any subsupplies from the provided company and the mechanism of subsupply and payment was only to conceal the bribe payment so that it would seem to be a legal payment within a business relationship; also, an alternative was agreed upon that if the bribe was paid to Ing. MF in cash, accused PC would invoice their services through an unidentified business company to the company L a.s., the invoicing would be accepted and financial resources paid, where accused PC from this company would obtain the money in an unidentified way and pay the amount of EUR 60,000.00 to Ing. MF.

6. The last serious criminal case when in 2020, a charge was brought for the criminal offence of receiving a bribe pursuant to Article 329 of the Criminal Code in concurrence with a criminal offence of legalisation of proceeds of crime pursuant to Article 233 of the Criminal Code, is the criminal case concerning the state-owned enterprise Lesy s.r.o.: In 2019, in the town of Banská Bystrica, Ing. TK, Ph.D. holding the position of Business Director of the company Lesy Slovenskej republiky, after a mutual agreement with Ing. LĎ, requested a bribe in cash from AJ for signing a Framework Agreement with J s.r.o. as a winner of a tender publicised in the Journal of Public Procurement, where the value of the bribe was set in the amount of 13% of monthly invoicing from the total contractually agreed amount in accordance with Framework Agreement 1607 amounting to €1,624,200 exclusive of VAT, and subsequently, in accordance with Framework Agreement 1608 in the amount of €2,120,600 exclusive of VAT, in the period from 31 March 2019 to 31 March 2020, a total amount of €122,253.59 was provided as a bribe; a part of the bribe was provided in cash in a passenger car (BMW X5) and a part through the company L P s.r.o., which legalised the bribes in the form of nine issued invoices in a total amount of €22,617.36 for fictitious consulting services between the companies J, s.r.o. and L.

It is obvious from the above list of the current serious criminal cases that since 2019, the number of criminal cases, in which particular high-level officials are criminally prosecuted, in most cases in detention, for corruption in concurrence with legalisation of proceeds of crime has considerably increased. It is caused by a more active approach of the police, as well as by the pressure created by the Prosecutor's Office on the police to focus on detection of more serious forms of corruption instead of dealing with minor corruption.

2.5.2. Forecast of ML threat development in corruption crimes

It is extraordinarily difficult to forecast the development of corruption in Slovakia, either focusing on ML threats or without them. All partial estimates of development of this type of criminal activities, which are based in particular on the analysis of already completed, i.e. detected and prosecuted acts, are not sufficient for the estimate of development in the future as they do not cover undetected corruption, which is much more extensive. Thus, it is possible to believe that the size and frequency of commission of these criminal activities will not change in future and will remain at the current level.

However, with respect to the development of criminal cases in 2019 and 2020, the forecast trend of detection and criminal prosecution or penalisation of this form of criminal activities is rising, and it can be expected that compared to 2016-2019, much more corruption cases in connection with legalisation of proceeds of crime will be detected and criminally prosecuted. If changes indicated above occur in the police (in particular strengthening the police with experienced analysts, operational staff and investigators, and completion of the proactive financial investigation mechanism), a considerable increase in such criminal prosecutions can be expected.

Taking into account the above-mentioned, it can be stated that the prognosis of threat of legalisation of proceeds of crime regarding corruption remains medium-high, and large systematic corruption will represent a real ML threat.

"Minor occasional corruption" cannot be considered a real ML threat in Slovakia, as the perpetrator of such act (e.g., doctor, policeman, office-holder) acquires in the form of bribe only an insignificant amount from the view of ML (maximum thousands of EUR), which does not need to be legalised in a sophisticated manner (normal consumption). A decreasing trend can be expected also as a consequence of civil society activities which increase the rate of resistance to the above corrupt behaviour.

2.6. Drug-related crime and so-called pharmaceutical criminal activity[31]

2.6.1. ML threat factors

As regards the generation of proceeds from drug-related crime and so-called pharmaceutical criminal activity, we can speak about a medium-high ML threat with an upward trend, where the assumed amount of unrecorded proceeds is substantially higher. Its organised form has the same character.

The transnational dimension is among the most significant aspects of drug trafficking and commission of drug-related crime.

[31] Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors Articles 171, 172, 173 (old Articles 186, 187)

The SR is a country with a fully developed domestic drug market offering all the drugs available in EU countries. Identically with the previous assessment period, as regards drug-related crime, the SR is still preferably a transit country or a temporary storage place for international drug traffickers.

Compared to the previous assessment period, the drug scene in the territory of the SR has not changed considerably. The development and trends copied the trends in the EU or of the global drug scene. The abuse of the internet for committing drug-related crime brings a lot of problems not only in connection with technological demands when detecting, documenting and investigating drug-related crime.

Drug-related criminal activities are a well-organised, lucrative and in particular latent form of criminal activity.

Perpetrators of drug-related crime are mostly Slovak nationals. However, international organised groups also operate in the SR, whose members have backgrounds in or come from south-eastern Europe. They organise production, import and distribution of narcotic and psychotropic substances in large volumes to the States of Western Europe, mostly marijuana and methamphetamine, but the activities of these groups also cover trafficking in cocaine from South America and heroin from Asia, or in substances with anabolic or other hormonal effects. These groups may be considered the largest ML threat from the groups committing drug-related crime in the SR.

Several types of narcotic and psychotropic substances, precursors and pre-precursors are transported most frequently by cars; however, also postal and courier services are abused for transportation. The ways of communication as well as concealment of criminal activities have not changed compared to the previous period; the state-of-the-art technology is used for communication, such as Internet, mobile phone, notebooks, smartphones, etc. Main communication means include Facebook, WhatsApp, Viber and similar applications, which hinders drug-related crime clarification to a great extent. However, dead drops are also used.

The most common way of drug-related crime commission in the SR is that people on top of the drug chain pyramid ensure the financing of purchase of great amounts of narcotic substances in the SR or abroad, in particular in the territory of the Czech Republic. Through other people, they ensure the transportation and storage of these substances at various places, from where they are distributed to end consumers or to entertainment facilities in other regions. The **profit/proceeds are then divided** according to agreed rules **among individual units involved in this illicit trade**.

Most perpetrators are also drug consumers; in principle, drug distributors at a higher degree of hierarchy do not consume drugs. Some persons dealing with drug-related criminal activities are linked to people working in healthcare, pharmacy or chemical industry, and through these people medicines, chemicals and other drug precursors needed for the production of methamphetamine circulate. Drug-related criminal activities are connected in particular with groups of perpetrators committing criminal offences against property and criminal offences of economic nature in order to obtain financial resources for the purchase of drugs and legalise proceeds of drug-related crime.

The drugs most widespread and used in the territory of the SR are cannabis /marijuana/, methamphetamine, followed by cocaine, heroin, synthetic drugs and new psychoactive substances. The most frequent ways of use are smoking, snorting and intravenous use.

Marijuana and methamphetamine are imported from abroad, in particular from the Czech Republic, where the perpetrators are people studying, working or living in the Czech Republic.

As regards marijuana, the quantity of substance imported ranges from quantities for personal use to the import of larger volumes for sale to several consumers. Groups of perpetrators cooperating with foreign groups also operate in the territory of Slovakia; in such case, modus operandi is more sophisticated.

Within the SR, methamphetamine was produced mostly individually, by consumers without sufficient financial resources for purchasing the drug. There are also manufacturers, who besides personal consumption sell the drug to several people close to them. In Slovakia, methamphetamine is prepared from over-the-counter medicines (e.g. Nurofen Stop Grip, Modafen and ParalenGrip), whose sale is, however, limited by law according to the number of packs needed for one treatment cycle.

As regards trafficking in heroin, Slovakia is a transit country rather than a target one. The reason for a low interest in heroin is its low quality at street sale, as well as the fact that current consumers of narcotic and psychotropic substances prefer substances with stimulating effects, in particular in the form of pills.

Trafficking in cocaine in the territory of Slovakia is an activity of organised groups, as well as smaller groups of individuals using cocaine. The imported cocaine came from the Netherlands or Belgium and its concentration was 80% or more. Cocaine is imported to the territory of Slovakia usually through an intermediary – a contact person or distributor from countries of South America.

Synthetic drugs and new psychoactive substances are imported to Slovakia mostly from the Netherlands, Poland, as well as the Czech Republic, or they are purchased via the internet. As a consequence of an increasing addiction to narcotic and psychotropic substances, as well as of lack of finances, many consumers get involved in drug-related criminal activities, either in the distribution or in the production and transportation of these substances. In the cases of import of cocaine, synthetic drugs and new psychoactive substances, the consumers interested pool their money for a certain quantity of goods, which are afterwards purchased abroad.

In 2018, the PF dismantled three organised groups and one criminal group. The persons of interest from the States of former Yugoslavia or the Albanian community carried out their activities in connection with trafficking, mostly in cocaine. Slovak nationals were involved mainly in the production and distribution of methamphetamine and Cannabis plants.

In 2019, a **sophisticated scheme created for the purpose of legalisation of generated proceeds of crime** – trafficking in substances with anabolic or other hormonal effects - was recorded. By mutual agreement and in coordination, in order to conceal such illegal income, at

least six perpetrators opened bank accounts at various banking institutions or used already existing banking accounts, to which they received cashless payments for supplies of substances with anabolic or other hormonal effects from various customers, transferred high amounts among accounts, withdrew cash and further disposed of these illegal funds. To improve the efficiency of the legalisation scheme, the perpetrators established business companies in the USA at one registered office and opened or ensured opening of three bank accounts of these companies in Slovakia holding the right of disposal of them; these accounts were used to transfer financial resources. In 2017, one of the perpetrators, a barrister, established through an intermediary – a company in the USA – another business company with a virtual registered office without real commercial and business premises; the position of Executive Officer of the company was held by the organiser of the group, and through an account in Slovakia, financial resources for the sale of substances with anabolic or other hormonal effects were further transferred, and the perpetrators intentionally carried out several transfers in order to conceal the origin of the money with a total volume of financial operations of at least EUR 17,560,240.00.

The perpetrators used these illegally obtained funds to commit other drug-related criminal activities, invested them in various consumer goods including the purchase of at least five passenger premium-brand motor vehicles and one utility vehicle, the purchase of six apartments, a part of the funds was transferred to tax havens; in order to improve the efficiency of legalisation and create a semblance of legal reason for the receipt of an amount of EUR 1,641,332.00, they provided a **fictitious loan contract allegedly concluded in August 2017, for an amount of EUR 2,000,000.00**. In this case, in accordance with Article 119 (1) (f) of the Code of Criminal Procedure, **"financial investigation" takes place focused on the evaluation of the whole property of the accused persons, their proceeds of crime and means to commit it, their location, nature, state and price. Cash amounting to GBP 21,200.00 and EUR 83,500.00, at least EUR 171,500.00 at bank accounts in the SR, as well as the whole property of the group organiser and the property of two accused legal persons, together in the value of at least EUR 1,413,000.00 have been seized so far.**

2.6.2. Drug prices and purity

Drug prices and purity in the territory of Slovakia are ascertained based on operational information of police members. In 2016, drugs with black market value from EUR 409,814.00 (lower limit) to EUR 1,257,210.00 (upper limit) were seized in the territory of the SR.

Development of prices of narcotic and psychotropic substances in the territory of the SR in the assessed period in EUR:

	2016	2017	2018	2019
Methamphetamine (Pervitin) /1 gram	35-100	35-100	20-100	20-100
Cannabis / 1 gram	5-10	5-15	3-20	2-20
Hashish / 1 gram	10-20	10-20	8-30	5-13
Cocaine / 1 gram	70-140	60-120	40-120	40-120
MDMA (ecstasy)/ 1 pill	3-12	3-12	5-15	3-12
Heroin / 1 gram	40-100	40-100	20-100	20-100

The above prices are not the average prices but the lowest and highest prices recorded in the territory of whole Slovakia for the whole year.

An increase in proceeds from drug sale is ensured by mixing them with other substances, so-called **drug cutting**[32].

In the monitored period of 2016 to 2019, in total 6,153 drug-related crimes were detected which represents a share of 2.40 % in total criminality. Compared to the previous monitored period of NRA, there was a decrease by 3,240 criminal offences. However, it should be noted that in the 1st round of NRA, the monitored period lasted five years, in the 2nd round, four years. Of the total number of detected drug-related criminal offences, there were 3,657 cases of convictions (a share of 59.43 %), and in 39 cases, the penalty of forfeiture of a thing was imposed, in five cases, the penalty of forfeiture of property, and in eight cases, the protective measure of confiscation of a thing. In particular cooperation in law enforcement, increased activity in the area of detection of illicit production and distribution of drugs and precursors, strengthened international cooperation in dismantling international organised groups contributed to the decrease in the number of drug-related criminal cases.

As regards the security situation in our territory, in the area of narcotic and psychotropic substances and precursors, **factors connected with secondary** criminality, i.e., criminal offences committed to obtain drugs, as well as criminal offences committed under the influence of drugs, must be taken into account in addition to illicit production, distribution and transportation of these substances.

Illicit income from drug-related crime of transnational Balkan crime comes in particular from countries of Western Europe. In Slovakia, it is legalised through related business companies under the influence of cooperating persons with both foreign and Slovak origin[33].

In the monitored period, illicit income was legalised through transactions with real estate, cryptocurrency, precious metals (purchase of gold as an investment and its storage in bank deposits in EU countries), investments in gambling venues, and a part of resources was invested to maintain and develop drug-related criminal activities. Illicit profits are also invested in the countries of the Western Balkans, where top representatives of this organised crime also have political coverage (in particular in Kosovo).

---

[32] *Heroin* in a mixture with opiates - Tramadol, Codeine (Braun), as well as with cheaper drugs, such as methadone... we also know a mixture of cocaine and heroin (speedball) Other substances may include: caffeine, glucose, chalk, talc.
Cocaine often mixed with codeine, lidocaine, oxazepam, diazepam, with other drugs such as heroin (according to the market price), powder, baking powder (Crack a form of cocaine – ammonia and dough conditioner)
Methamphetamine – it is often already produced as a mixture containing organic solvents (toluene, gasoline, benzene, acetone or iodine, etc. It is also mixed with other stimulants, sugar, salt, cyclohexanone, washing powder, pulverised dishwasher tablets, etc. In mixtures with heroin (speedball).
MDMA (ecstasy) mixed with Piperazine (mCPP) – a substance causing depression, gypsum, other powdered substances, medicines regulating heart activity, often several types (i.e., including opposite effects on heart).

[33] Representatives of foreign organised crime have been trying to obtain permanent residence in the SR or the SR's nationality for a long time. In addition to the possibility of free movement in European Union States, they also try to obtain the possibility to organise their illicit activities in the territory of Slovakia or to legalise proceeds of crime committed abroad in Slovakia through their legal business activities.

A phenomenon of the current era, the **Darknet**, which provides room for illicit activities committed via the internet, continues to be used for the commission of drug-related crime. Illicit activities are difficult to monitor because the internet is a global environment and it is difficult to identify organisers of trafficking due to constantly changing IP addresses of traffickers. Orders placed via internet sales portals usually include smaller amounts of drugs delivered by post or courier services.

2.6.3. Forecast of ML threat development in drug and pharmaceutical crime

Based on the development it can be expected that **cannabis and methamphetamine consumption,** including their production, import, distribution, as well as an interest in precursors necessary to produce methamphetamine, will further increase.

An increase in consumption of new psychoactive substances connected with their procurement **via the internet and abuse of courier and postal services for their import** can also be expected. There is also an assumption of stagnation of interest in traditional heroin connected with an increase in the interests in synthetic opiates and opioids contained in medicines, as well as the involvement of groups of perpetrators coming from the Balkan Peninsula in trafficking in heroin and cocaine in the SR. Like in other countries of the European Union, an increase in the interest in the so-called "laughing gas" can also be expected.

Currently, an increasing interest of some groups of the population and civic associations in a change of the legislation in the area of narcotic and psychotropic substances, e.g., exclusion of LSD etc., as well as an increased interest of socially vulnerable people in particular in Eastern Slovakia in solvents[34], as they are affordable, is expected. A greater influence of organised groups, whose members operate in various other countries and deal with trafficking in narcotic and psychotropic substances and precursors, as well as alteration of organised groups dealing with drugs, is very probable.

The Slovak Republic will continue to be considerably affected by the regional factor of drug-related crime.

2.7. Organised crime

2.7.1. ML threat factors

The level of ML threat in the cases of organised forms of criminal activity remains high, especially with respect to the volume of generated proceeds, volume of unidentified proceeds, nature, social hazard and scope of related criminal activities in predicate criminal offences with a balanced tendency, however, with the transformation in the area of specific criminality with a considerable shift to criminal offences of economic nature.

The Slovak law does not know the term "organised crime", therefore, it occurs in connection with other criminal offences which are committed or were committed by members

[34] These are organic-solvent-type drugs which are inhaled (acetone, toluene, chloroform, etc.).

of organised or criminal groups. Usually, it is not one definite fact or summary of facts; rather it is a complex form of devious conduct showing signs of unlawfulness with a high degree of hazard for the society. **As regards facts, organised crime is heterogeneous.**

As in the previous assessment period, in the second assessment period, too, the trend prevailing in the territory of the SR was that **criminal and organised groups** desist from mostly criminal violence and criminal offences against property, and their **illicit activities** move towards more sophisticated and profitable forms, which are more complicated for detection and conviction of the perpetrator. This includes in particular **criminal offences of economic nature, drug-related crime and criminal offences against property**.

The criminal offences of economic nature included **frauds with EU funds and in particular tax criminal offences**, in particular in the form of issuance of fictitious accounting and tax documents for a great number of various business companies without real taxable transactions with the objective of unauthorised tax advantages in the form of tax liability evasion and unauthorised application and subsequent refund of excess value added tax deduction. **An international element and abuse of schemes of legal persons** were used to avoid a suspicion of commission of criminal activities as well as to make the activity of criminally liable persons more obscure.

In the monitored period, a case of a particularly serious criminal offence of legalisation of proceeds of crime was detected. The perpetrators of the predicate criminal offence of establishing, masterminding and supporting a criminal group pursuant to Article 296 of the Criminal Code and a particularly serious criminal offence of theft pursuant to Article 212 (1), (5) (a) of the Criminal Code allegedly unlawfully had taken possession of a majority interest in a foreign company and at the following extraordinary general meetings of the foreign company, they decided on the liquidation of the company and on reducing its registered capital. In order to thwart the seizure of the acquired financial resources from the reduced registered capital for the purposes of criminal prosecution, they legalised them by concluding contracts of purchase of other shares in other foreign companies or by providing loans to related persons, both Slovak and foreign companies in a total amount of about EUR 4,527,325.75.

Official spheres of business of organised crime members focus on the protection of property and persons performed through private security services, sale and purchase of real estate, operation of hotels, restaurants, gambling venues, exchange offices, as well as provision non-banking loans; the area of tax criminal activities with elements of cooperation with organised groups of in particular neighbouring countries is becoming ever more dominant.

If any of the criminal groups committed criminal violence, it was only for the purpose of control of some area of criminality in a small region (town, district), with the objective to collect fees from drug dealers or persons committing criminal offences of economic nature or criminal offences against property. Therefore, Slovak authorities endeavour to detect such newly established organised or criminal groups still at early stages, document their criminal activities and dismantle them.

In the SR, no serious unlawful activities of foreign-language criminal groups were recorded, but it is a more frequent phenomenon seen in individual criminal cases that criminal

activities exceed state borders, in particular in the cases of organised drug-related crime, prohibited acquisition and possession of firearms and trafficking in them, and the so-called pharmaceutical criminality, where despite the development, organised crime still persists.

In the assessed period of 2016 to 2019, no profiling of new organised or criminal groups was recorded, which would have such dominance of position in the region that it would raise concerns about the commission of severe criminal violence like the violence committed in the previous years by groups of racketeers that were eliminated in the past.

In the assessed period, the "Takáč" criminal group was dismantled; its structures were more sophisticated than in other groups, i.e., they desisted from violent elements and replaced them by contractual obligations. They did not use proceeds of crime for consumption; they invested them in particular in the sector of services (e.g., restaurants, hotels). This elimination also results from 2016, when criminal activities of nine criminal groups and 49 organised groups were documented; out of them, 26 organised groups and four criminal groups were dismantled. As regards organised drug-related crime with an international element, five organised groups were documented; two of them and one criminal group committing drug-related crime were dismantled.

In the assessed period, policemen from NAKA PPF actively operated in the area of fight against criminality of criminal groups operating in the territory of the Slovak Republic; they clarified several cases of "mafia murders", i.e. murders causally connected with the activity of criminal groups or commission of the most serious forms of organised crime. They include the clarified cases of "mafia execution of straw men". These acts were cleared up despite the fact that the investigation was hindered due to a considerable time delay between the commission of the act and detection of the perpetrator (about 10 and more years).

In the monitored period, in connection with the investigation of activity of organised groups and criminal groups, 279 persons as members of 24 criminal groups and 434 persons as members of 83 organised groups were charged. Investigation of five so-called mafia murders committed from 2000 to 2004 by the "Sátor" criminal group continued; all the accused perpetrators are prosecuted in detention. In October 2019, within the "Apač" operation, 19 members of the "Takáč" criminal group were arrested, 13 of them are prosecuted in detention and 25 persons were charged.

Legalisation of proceeds of crime by organised or criminal groups is often masked as legal income from regular business activities.

For that purpose, organised groups operate various businesses, such as gambling venues, restaurants, shops, exchange offices, etc., where small cash amounts are often handled. Proceeds of crime are often put into the legal financial system through extensive financial operations among many legal and natural persons for the purpose of concealment of financial proceeds. Subsequently, organised groups invest these sham legal financial resources in various commodities, such as real estate, securities, or provide various types of loans.

Law enforcement authorities realise the need to improve the efficiency of application of mechanisms of detection and confiscation of proceeds of crime, as well as property acquired

using illicit proceeds, however, on the other hand, it should be noted that a **lower efficiency of prosecution of cases of disposal of proceeds of crime consists in particular in insufficient and unclear definition of the boundary between a plain disposal of proceeds and a qualified intention of legalisation in accordance with Article 233 (1) of the Criminal Code.** Law enforcement authorities in criminal prosecution, as well as courts in practice often face defence of the prosecuted persons (accused persons), which can be rebutted with difficulty, that the disposal of proceed (transfer to their accounts and accounts of close persons or cash withdrawals) was essentially the consumption of proceeds from a predicate criminal offence, without an intention to conceal their origin, which disputes the culpability of the act legally qualified as a criminal offence of legalisation of proceeds of crime. There is also another important factor – problems of interpretation caused by a complex distinction made between facts of criminal offences of sharing pursuant to Article 231 of the Criminal Code and legalisation of proceeds of crime pursuant to Article 233 of the Criminal Code; in consequence, the perpetrator is more frequently prosecuted and convicted of the criminal offence of sharing (Article 231 of the Criminal Code), which is virtually a form of the so-called autonomous money laundering (third party laundering) than of legalisation of proceeds of crime (Article 233 of the Criminal Code).

The ML threat persists in the area of human smuggling, also with respect to the volume of unidentified proceeds generated by this criminal activity.

The activity of organised crime also focuses on criminal activities of **human smuggling pursuant to Article 355 and Article 356 of the Criminal Code**.

As in the previous assessment period, the area of human smuggling in Slovakia was most significantly affected by the migration wave from the countries of the Western Balkans from 2015-2017, which went through Slovakia from Hungary and then divided in the direction of the Czech Republic, Austria and Poland. After 2017, the migration pressure has weakened, which was reflected by the number of human smuggling cases on the route of illicit migration. At the end of 2019 and the beginning of 2020, as a consequence of a strained political situation between the EU and Turkey, the pressure of illicit migration increased on the border between Turkey and Greece, causing a slight increase in migration pressure on the migration route of the Western Balkans, however, it did not reach the intensity from 2015-2017.

Economic migrants from countries unaffected by a conflict, who arrive in Ukraine, obtain illegal documents and try to get into the EU using them. Migrants are smuggled by Ukrainian or Ukrainian-Slovak organised groups cooperating with security units on both sides of the border. The price for the transfer of one migrant across the border between Ukraine and Slovakia is about USD 3,500.00.

As regards illegal migration after 2016, we can see a considerably stronger interest of third-country nationals in obtaining residence in the Schengen Area, as well as in illegal border crossing, which is also proved by the changed status of Slovakia from a solely transit country to a target country. Entities dealing with obtaining temporary residence permits for the purpose of business operate in Slovakia. For the services provided, they receive an amount of EUR 3,500.00 to 7,000.00 from every person, depending on the difficulties with residence permit obtaining. Some entities also provide other services to foreigners, such as establishment of

companies, bookkeeping, formal conduct of business activities so that foreigners seemingly meet the criteria for granting a temporary residence permit although they in fact do not stay or run a business in the SR. To obtain residence permit, also marriages with Slovak nationals are arranged; based on them, foreigners apply for residence for the purpose of family reunification. In the cases of family reunification abuse, Slovakia used to be a source country of brides or bridegrooms who were often lured abroad, in particular to Great Britain, with the promise of a well-paid job and later they agreed with marriages with third-country nationals. Gradually, the arrangement of contract marriages also started in Slovakia. However, in 2019, the trend started decreasing again.

High demand for work in Slovakia by third-country nationals, in particular from Ukraine and Serbia, was used by groups knowing foreigner legislation; covered by HR agencies and various business companies, they fraudulently obtained necessary documents for applicants for residence and job in Slovakia.

In the area of human smuggling in Slovakia, a very low level of money laundering has been recorded because main revenues and main cash flow from human smuggling are not situated in and transferred through Slovakia. In most cases, the activity of organised human smuggling groups is managed from abroad and the members performing activities in Slovakia are paid only partial considerations for services by main organisers. In some cases, illicit migrants pay for the transportation directly to drivers. The financial resources obtained for individual services (e.g. transfers of migrants) are either paid in cash or deposited into current accounts of members (e.g. the amounts for accommodation, fees for handling foreigner matters). The financial proceeds are further used for the provision of services intended for the coverage of business activities or invested in motorsport or accommodation companies. Members of organised groups usually use the proceeds of activities for personal needs or a part of the resources is paid as wage to illegal migrants working in Slovakia.

As regards ML, business companies reporting fictitious activities with fictitious accounting with the only objective to obtain residence permits for foreigners from third countries for a financial fee appear as the riskiest ones in the area of human smuggling.

Sophisticated serious organised criminal activities are dominantly characterised by **a concurrence of several criminal offences.**

In the monitored period from 2016 to 2019, in total 218 criminal offences committed by organised and criminal groups were detected, which represents 0.09 % of overall criminality.

Commenced criminal prosecution for criminal offences committed by organised groups					
	2016	2017	2018	2019	2016-2019
Premeditated murder Article 144	3	0	0	0	3
Murder Article 145	0	0	0	0	0
Bodily harm Article 155	0	0	0	0	0
Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors Article 172	14	6	6	8	34

Unauthorised handling of substances with anabolic or other hormonal effects Article 176	0	0	0	1	1
Trafficking in human beings Article 179	2	1	0	0	3
Kidnapping for ransom Article 186	0	0	0	1	1
Robbery Article 188	2	1	0	0	3
Extortion Article 189	2	1	0	0	3
Gross coercion Article 190	0	0	0	0	0
Theft Article 212	2	3	1	3	9
Fraud Article 221	3	4	1	1	9
Insurance fraud Article 223	23	0	0	0	23
Sharing Article 231	0	0	0	0	0
Legalisation of income from crime Article 233	0	0	0	0	0
Harm caused to a creditor Article 239	0	0	0	0	0
Breach of regulations governing imports and exports of goods Article 254	0	0	0	0	0
Forgery, fraudulent alteration and illicit manufacturing of money and securities Article 270	0	1	0	0	1
Tax and insurance premium evasion Article 276	7	7	8	3	25
Failure to pay tax and insurance premium Article 277	1	0	0	0	1
Tax fraud Article 277a	4	7	1	1	13
Breach of regulations governing state technical measures for labelling goods Article 279	0	0	0	1	1
Prohibited acquisition and possession of firearms and trafficking in them Article 294	0	1	1	0	2
Prohibited acquisition and possession of firearms and trafficking in them Article 295	0	0	0	0	0
Establishing, masterminding and supporting a criminal group Article 296	0	0	0	2	2
Illicit manufacturing and possession of nuclear materials, radioactive substances, hazardous chemicals and hazardous biological agents and toxins Article 298	0	0	0	0	0
Abuse of power by a public official Article 326	0	0	0	0	0
Receiving a bribe Article 329	0	1	0	0	1
Obstruction of justice Article 344	0	0	0	0	0
Human smuggling Article 355	1	1	1	0	3

Human smuggling Article 356	1	0	0	0	1
Old Criminal Code	0	6	0	3	9
OVERALL CRIMINALITY	66	43	25	26	160

Commenced criminal prosecution for criminal offences committed by criminal groups					
	2016	2017	2018	2019	2016-2019
Premeditated murder Article 144	1	0	4	1	6
Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors Article 172	0	0	0	4	4
Kidnapping for ransom Article 186	0	0	0	0	0
Robbery Article 188	0	0	0	0	0
Extortion Article 189	1	0	0	0	1
Gross coercion Article 190	2	1	0	0	3
Fraud Article 221	0	0	0	2	2
Insurance fraud Article 223	0	0	0	0	0
Sharing Article 231	0	0	0	0	0
Legalisation of income from crime Article 233	0	1	0	0	0
Harm done to a thing of another Article 245	1	0	0	0	1
Breach of regulations governing imports and exports of goods Article 254	0	0	0	0	0
Distortion of data in financial and commercial records Article 259	0	0	0	0	0
Forgery, fraudulent alteration and illicit manufacturing of money and securities Article 270	0	0	0	0	0
Tax and insurance premium evasion Article 276	1	2	2	1	6
Failure to pay tax and insurance premium Article 277	0	1	1	0	2
Tax fraud Article 277a	0	0	0	0	0
Prohibited acquisition and possession of firearms and trafficking in them Article 294	0	2	0	0	2
Prohibited acquisition and possession of firearms and trafficking in them Article 295	1	1	0	0	2
Establishing, masterminding and supporting a criminal group Article 296	3	5	9	1	18
Abuse of power by a public official Article 326	0	0	0	0	0
Old Criminal Code	0	5	2	1	8
OVERALL CRIMINALITY	10	18	19	11	58

2.7.2. Forecast of ML threat development in organised crime

It can be expected that criminal activities generating the biggest volumes of illicit proceeds, such as tax (in particular VAT) frauds, illicit import/smuggling of high-tax goods, asset stripping in state-owned institutions and local and regional government, corruption in selecting suppliers and issuing various licences and assigning subsidies, and in the area of drug production and trafficking will step up.

The migration pressure on the external border of the EU considerably decreased, in particular thanks to the fulfilment of the so-called migration agreement between the EU and Turkey and introduction of stricter security controls on the borders of countries in the Western Balkans. However, the migration agreement became a risk tool of Turkey for the enforcement of concessions of the EU. Its termination cannot be excluded in particular due to the increasing requirements and even aggressive behaviour of Turkey towards EU Member States. The above factors may increase the threat of illicit migration across the Schengen/Slovak border with Ukraine and also illicit profit of smuggling groups on both sides of the border. At the same time, an increase in illicit proceeds for Slovak entities arranging temporary residence for foreigners in the SR, in particular for the purpose of business, can be expected (although, as a matter of fact, this does not happen and foreigners often migrate to western countries of the EU). The closer connection of Ukraine and Georgia, as well, within the Eastern Partnership to the European economic and political area brings cancellation of visa duties by the EU and intensification of economic and business links among these countries.

There is a big problem with forecasting the state, level, structure, and dynamics of organised crime at least due to the absence of a legal definition of the term "organised crime". The factors, which will support organised criminal activity in the SR, will include in particular difficult taking of evidence, and organised groups will also focus on new forms of abuse of legal persons.

The organised form of crime represents a permanent ML threat with unchanged amplitude of trend, however, with a significant change of character of criminal activities towards economic criminal activities.

2.8. Cybercrime

2.8.1. ML threat factors

Cybercrime in the Slovak context represents a dynamically developing type of criminality. The most serious forms of cybercrime represent a medium-high ML threat with a rising tendency but also rising clear-up rate. The proportion of unrecorded proceeds is substantially higher. The recorded attacks in cyberspace outmatch traditional criminal activities and become a horizontal element of it. The existence of virtual currencies represents a special threat with a tendency of growth.

The term "cybercrime" is not defined in Slovak law, however, Slovak law knows and defines facts of individual criminal offences which together form cybercrime. At the same time,

for the purposes of the Slovak criminal law practice, definitions such as "computer system" and "computer data" contained in the Convention of the Council of Europe[35] ratified by the SR on 12 December 2007[36] are used.

The categorisation of cybercrime in a narrower sense (direct cybercrime) has not changed and includes attacks on computers, i.e., unlawful activities carried out against the integrity or security of computers, computer systems or data that is processed or stored. On the contrary, cybercrime in a broader sense (indirect cybercrime) means in this assessment period too, the criminal offences committed by means of computer (a computer as the means for criminal offence commission), i.e., any unlawful activities committed through computer systems or computer networks. They include in particular criminal offences of economic nature, such as frauds, thefts, computer sabotage or illicit penetration into computer networks and to protected data. They also include criminal offences attacking an individual's privacy (modification of personal data, use of false data, illicit collection or abuse of personal data), however, they are also used in committing other criminal activities, related, for example, to extortion, threats, dissemination of child pornography and drug-related crime.

The clear-up percentage of criminal offences within cybercrime is also considerably affected by the fact that in particular PF members in charge are competent for the investigation of this form of criminal activity in basic facts of investigated criminal offences; however, in most cases they are not sufficiently experienced. The low clear-up rate of cybercrime is strongly related to the development of new information technologies and services with the use of various sophisticated ways in the environment of P2P/TOR networks, social engineering, etc. The missing legal regulation, which would lay down the telecommunication service providers' duty to store data, is a significant problem. This situation results from the practice of the Constitutional Court of the SR and the Court of Justice of the EU. Although perpetrators of this criminal activity are more and more sophisticated and the situation is similar as regards the scope of use of new technologies, currently, even the data available in 2014 is not available any more. A new efficient legislation at the level of the EU can be hardly expected due to narrow room for a legislative regulation by the Court of Justice of the EU.

Electronic evidence, which represents the basis for successful investigation of cybercrime, is characterised by high volatility. Without timely seizure of clues and evidence, there is only small or no success rate of detection, detention and conviction of perpetrators. The cross-border character is among the typical signs of cybercrime.

The problem of solution of internet criminality in general in all its known forms at all degrees of gravity remains the most serious threat. To be able to speak about cybercrime, the perpetrator must use computer technology or another means for information processing for their activity, and their activity must fulfil the fact of criminal offence.

In the 2nd round of NRA, **the biggest share of cybercrime occurrence was represented by criminal offences in the area of abuse of payment cards**. Within the assessed period, in 2016, the highest damage was recorded, amounting to EUR 1,352,000.00. As regards

[35]Convention on Cybercrime of the Council of Europe of 23 November 2001

[36]Computer Crime or Cybercrime is specified by the European Commission and European Union Member States: "Cybercrime is any illicit, immoral and unauthorised conduct including the abuse or change of data obtained through computer technology."

the development of damage, it was stabilised or slightly decreased compared to the previous assessment period. This criminal offence is the most frequently committed cybercrime criminal offence and represents on average, a share of about 78 %.

The number of criminal activities conducted directly against information systems (damaging and abusing a record on an information carrier - Article 247 of the Criminal Code and other criminal offences) **increased** in the assessed period. This criminal activity resulted from the continuing rise of use of information technologies, in particular in households. In the assessed period, **an increase in the dissemination of child pornography** was also recorded**, mainly thanks to the possibilities of anonymity and untraceability. Distribution of materials with child pornography was and is most frequently recorded at internet chat portals and internet forums. Within this criminal activity, we do not register the generating of proceeds of crime because perpetrators of these criminal offences are usually recipients of these services and products, whose motive is sexual satisfaction rather than profit, therefore, often the scenario is opposite, when perpetrators pay for it.**

Overview of cybercrime criminal offences[37] for the monitored period 2016 – 2019:

	Year	Article 201a	Article 219	Article 247	Article 283	Article 368	Article 369	Article 370
Occurrence	2016	5	1741	17	41	30	100	27
	2017	11	1579	26	44	29	174	28
	2018	15	1537	23	46	36	234	54
	2019	13	1368	29	47	60	191	35
Cleared-up	2016	1	433	0	8	17	32	21
	2017	8	451	0	11	15	48	19
	2018	6	473	0	10	25	76	38
	2019	6	492	4	14	42	58	24
Clear-up percentage	2016	20.00	24.87	0.00	19.51	56.67	32.00	77.78
	2017	72.73	28.56	0.00	25.00	51.72	27.59	67.86
	2018	40.00	24.87	0.00	21.74	69.44	32.48	70.37
	2019	46.15	35.96	13.79	29.79	70.00	30.37	68.57
Damage (thous. EUR)	2016	-	1352	38	122	-	-	-
	2017	-	919	104	246	-	-	-
	2018	-	1268	116	181	-	-	-
	2019	-	1065	250	2146	-	-	-

[37] The form of criminal offence as the basic statistical instrument does not contain an item whether the criminal offence was committed via a computer. For that reason, cybercrime includes the criminal offences provided in the table: Article 201a Sexual abuse, Article 219 Unlawful manufacturing and enjoyment of payment means Article 247 Unauthorised access to a computer system, Article 283 Infringement of copyright, Article 368 Production of child pornography, Article 369 Dissemination of child pornography, Article 370 Possession of child pornography and participation in child pornographic performance.

The development of the fight against cybercrime in 2016-2019 was considerably affected by Decision of the Constitutional Court of the Slovak Republic No. US 10/2014 dated 29 April 2015, which decided that the provisions of Article 58 (5) to (7) and Article 63 of Act No. 351/2011 Coll. on electronic communications as amended, Article 116 of the Code of Criminal Procedure and Article 76a (3) of Act of the National Council of the Slovak Republic No. 171/1993 Coll. on the Police Force as amended **are not** in compliance with Article 13 (4), Article 16 (1), Article 19 (2) and (3), and Article 22 of the Constitution of the Slovak Republic, Article 7 (1), Article 10 (2) and (3) and Article 13 of the Charter of Fundamental Rights and Freedoms, Article 8 of the Convention on Human Rights and Fundamental Freedoms and Article 7, Article 8 and Article 52 (1) of the Charter of Fundamental Rights of the European Union. It is also considerably affected by the continually adopted case law of the Court of Justice of the EU.

ML threats related to the use of information and telecommunication technologies (including social networks and online payment platforms), internet banking etc. can also be seen in the 2nd round of NRA for criminal offences of economic nature and criminal offences against property. Other forms of criminal activities committed by means of computer system, e.g., extortion etc., cannot be neglected.

These technologies allow not only efficient and fast communication and transfer of funds (including the cross-border transfer) within common legally provided services but also commission of criminal activities.

Encryption of communication as a clear trend facilitates the commission of criminal activities. **Phishing[38], pharming[39], use of malware and ransomware are still present.**

In such cases, legalisation proceedings do not take place very often because it is often almost impossible to investigate even the predicate criminal offence or the act of legalisation is subsumed in the predicate criminal offence, for which the criminal prosecution takes place. For example, in the cases of frauds, where the perpetrator fraudulently notifies a change of bank account for invoice payment and the injured person finds out that it is a fraud and files a criminal complaint, the financial resources have already been withdrawn or transferred and computer data cannot be retrieved because the operators' duty to store data for a certain time is missing.

[38] The cases when a personal computer or mobile phone of an owner of a particular account was intentionally attacked by software – virus, through an SMS message or by a fraudulent application for the purpose of subsequent unauthorised transfer of money from the selected account without the account holder's knowledge and consent. Some of them even looked as if sent by the bank itself. Subsequently, the injured person's bank account was debited.

[39] There were abuses of access to injured persons' accounts; being sure that they carry out common operations on their accounts via internet banking, the account holders were redirected by an unauthorised intervention without their knowledge from home websites of their banks to false sites which at first sight were not different from the genuine domains. In this way, the injured persons involuntarily provided the unauthorised person with protective and security elements for internet banking, which provided perpetrators with free access to their accounts and they used it subsequently to fraudulently withdraw financial resources in cash.

Taking into account that **these ML threats and risks do not have a local character but a cross-border one** connected with global spread and availability of internet, these threats and risks require an international approach both at the level of FIUs and banking systems, however, they also require **cooperation with the providers of telecommunication services (including social networks).**

The primary obstacles to successful investigation of cybercrime include the absence of the duty of the providers of telecommunication services and social networks to save a defined scope of data for a certain period, which can only be overcome by EU legislation, and in this context, a longer period of execution of international judicial cooperation (in particular in relation to operating and content data). The examples of impacts of this situation include the fact that at the time when data is provided from abroad and lead, for example, to a Slovak IP address, it cannot be really used because the Slovak providers do not keep the data anymore. Finally, insufficient experience of the PF members in charge in investigating less serious forms of such criminal activity also should be noted here.

In this context, the current state of data storage in the European Union is a significant threat.

2.8.2. Other forms of related cybercrime with an ML threat

In addition to the most widely known forms of computer piracy and cybercrime, we also encounter more sophisticated procedures.

Cases were recorded, where **a payment card was abused** either after physical theft or after card identification data were acquired illicitly and abused.

There were various forms of fraudulent activities, e.g., the installation of a camera at an ATM in order to obtain the PIN security code, calling a customer in order to obtain access data to the bank account etc. By acting so, perpetrators committed the criminal offence of **theft** pursuant to Article 212 of the Criminal Code, criminal offence of **embezzlement** pursuant to Article 213 of the Criminal Code or criminal offence of **fraud** pursuant to the provisions of Article 221 of the Criminal Code, etc.

In 2018-2019, cases of using malware, in particular keylogger and related forms, for unauthorised acquisition of customer data for various cashless payment services were recorded. Besides standard services, such as internet banking, the attacks of perpetrators are focused on the acquisition of identification and authentication data to accounts, such as PayPal, Skrill and other virtual purses (and services with a link to a payment card or current account).

Last but not least, attacks on databases of e-commerce entities (e-shops) should be noted, when a software attack on the trader's customer database containing data is performed; the data is subsequently abused for unauthorised transactions. Often it is a direct software attack on an e-commerce POS terminal and sniff data of payment cards, when perpetrators get to complete data of a customer and their payment card. The data is then distributed to third persons, who will perform the fraudulent transactions and obtain unlawful profit. The

booking.com domain has been attacked in such a way several times and data of several hundreds of customers of Slovak banks have leaked.

A form of commission of criminal offences of economic nature consisting in **"diverting of payments" or "CEO frauds" within a standard business payment system of business partners in large volumes (millions of EUR)**, which is used by perpetrators, also persists in the second assessment period.

CEO frauds are discussed in more detail in Chapter 2.4.4.5 Threats resulting from the abuse of Slovak business companies.

It is assumed that proceeds are generated in the Slovak Republic and placed abroad. This assumption can be verified only indirectly, for example, through the cases of international judicial cooperation, where requests for evidence concerning transfers of financial resources to bank accounts or crypto exchanges out of the territory of the SR were recorded. No statistical data on generating proceeds in the SR and placing in the SR is available.

2.8.2.1. Virtual currency

The ML threat resulting from the existence of virtual currencies is high with the tendency to grow also with respect to the scope of the unidentified volume of placed proceeds of crime.

The Bitcoin virtual currency is accepted by an increasing number of merchandisers. It can be exchanged through proven intermediators or exchanges, in a cashless way, with a certain time delay. Special bitcoin ATMs are another variant, there are 42 of them in the SR; however, they often offer only purchase and not sale, geographically, they cover the whole SR. In the assessed period, the Bitcoin virtual currency was also seized in two cases, it was subject to forfeiture to the State. In this context, there were several application problems regarding the application of the Code of Criminal Procedure related in particular to the terms of court decisions on the forfeiture, and subsequently to the issue of transaction costs; the practice also raised the need to create an internal regulation regulating the process of seizure and subsequent transfer of Bitcoin to an official purse of the PF in a uniform way for all units.

It should be noted that an increase in the use of **virtual currency** was recorded in the assessed period, which means that an increase in the risks connected with the development of these technologies both at the level of investigation and clarification of predicate criminal offences and at the level of confiscation of proceeds of crime can be expected. It should also be noted that among virtual currencies, in particular Bitcoin has become widespread in the assessed period; the other currencies were used to a minimum extent or were not used at all.

The Prosecutor's Office prepared a manual concerning virtual currencies for prosecutors which was updated in 2019 and is available on the intranet. The National Network of Prosecutors to Combat Cybercrime established in 2017 in close cooperation with the Cybercrime Department of the PPF SR also deals with this topic. Attention is also paid to this area through a representative of the Prosecutor's Office in the European Judicial Cybercrime Network, which prepares a manual for prosecutors and judges in this area.

In 2020, a phenomenon of social engineering (formerly known from other States) also expanded in the SR; in a sophisticated way, perpetrators use, for example, fictitious messages of problems with Microsoft products, etc., and then based on the obtained access to devices, they transfer financial means of the injured persons, in many cases these funds are converted into virtual currency and then disappear. The perpetrators call from phone numbers, which are generated automatically and often "look like" Slovak phone numbers. This is a global problem of insufficient regulation of telecommunications, when telecommunication companies are not able to solve the problem (the possibility of blocking such calls would require a global legislative and technical solution).

Despite a unique identification of means, virtual currencies allow the owner's anonymisation, which along with the possibility of laundering by exchanging creates an efficient obstacle to transaction tracking.

The Cybercrime Department has no tool to track transactions with virtual currency (e.g., Chainalysis), which represents a significant risk for efficient tracking of proceeds with the use of virtual currencies and suppression of fight against virtual-currency-related crime.

2.8.3. Forecast of ML threat development in cybercrime

In future, a high latency will be seen in cybercrime in committing criminal offences on social networks in cyberspace. Black economy is also on the rise; the volume, scope, and material damage committed by cybercrime will be high with a rising tendency.

The essential ML challenge is to provide for the preparation of staff and create technical conditions necessary to efficiently reveal it, including a new regulation of data storage by providers of services.

Some EU Member States, taking into account IOCTA 2016-2019 inform that the attacks recorded in cyberspace overcome the traditional criminal activities. The upward trend will be supported by both the increasing number of cybercrime and opportunities in these profitable illicit activities, as well as by the technological development of new instruments, for example, in frauds with ATMs or malware in mobile phones. There will be problems in particular with **poor security standards and practices of companies and individuals.** In accord with IOCTA Reports 2016-2019, in particular ransomware and malware appeared in the assessed period.

The Europol's report "Internet Organised Crime Threat Assessment" (IOCTA) from 2016-2019, however, also mentions some positive aspects. Cooperation between companies and law enforcement authorities gradually develops; it led to the revelation and destruction of several organised criminal groups and high-level individuals involved in child abuse, cyberattacks or frauds with payment cards. Social responsibility of ICT providers and service providers increases.

The rising trend of cybercrime and damage caused by these criminal offences was also confirmed by SOCTA 2017. The occurrence of cybercrime in the SR in the assessed period followed this trend only partially, when the documented damage in criminal offences related to abuse of payment cards increased.

2.9. ML threats from the view of SOCTA[40]

At least two highly professional and mobile organised groups operated in the territory of the SR in the assessed period; they focused on continuing criminal offences of ATM break-in with proceeds amounting to about EUR 707,000.00, and thefts after breaking in goldsmiths stores with proceeds amounting to about EUR 763,000.00.

According to SOCTA 2017, highly mobile organised groups focusing on break-in thefts will represent one of the main risks in the next period.

In the territory of the SR, continuing thefts were recorded, by breaking in ATMs after an explosion caused by compressed gas or using a black box[41] committed by an organised group from Moldova and Romania. The group committed the activity in the territory of the SR (and in Hungary, the Czech Republic and Germany) from 14 September 2017 to 19 November 2018 using explosions (hereinafter the "explosive attacks"). In the mentioned period, in total eight explosive attacks were committed in the territory of the SR, where an unknown substance with an unknown blasting agent was introduced through a supply hose into the ATM body. The clarification of other six explosive attacks resulted in a suspicion that they had been committed by an organised group of Moldova citizens with a total damage covering the stolen cash in the acts documented in the SR in the amount of EUR 707,480.00.

A series of continuing thefts by breaking in mainly in shopping centres was detected in the assessment period. In the period from 2 November 2019 to 3 September 2020, in the territory of the SR, six thefts were committed by breaking in jewellery stores (a part of them at a stage of attempt). It can be reasonably supposed that they were committed by a mutually coordinated organised group of perpetrators (citizens of Romania) operating in the territory of several States presumably using a logistic background (accommodation is assumed before and maybe after the act) in Hungary and taking various countermeasures in relation to the clarification of criminal activities (hereinafter the "countermeasures"). Modus operandi of all the thefts committed by breaking in jewellery stores consisted in general of the arrival of 5 – 8 (most frequently 6 – 7) perpetrators to the place of offence (only the numbers recorded by camera systems are mentioned, other persons could presumably also participate), getting through the emergency exit – by breaking the glass and after entering the shopping centre, breaking into the jewellery store after breaking the entrance door or break opening the protective lattice using hammers, axes, various metal and assembly rods. In all cases it was found out that the perpetrators had escaped without the use of transport means, by running to a distance of several hundreds of metres to several kilometres. The damage caused by stealing the jewellery (proceeds) in the acts documented in the SR amounts to about EUR 763,000.00.

[40] The last published data from 2017

[41] A form of a logical attack by connecting an ATM to an external device – black box able to change the basic algorithms and commands of the ATM related to cash withdrawal

2.10. Environmental crime[42]

2.10.1. ML threat factors

In assessing environmental crime, it can be stated that only some forms of environmental crime, in particular illegal activities with waste (illicit import, dumping and disposal), illegal trade in timber and illegal trade in endangered species of wild fauna and flora, have an extensive international dimension; this criminal activity includes high financial proceeds.

Environmental crime means the criminal activity, where the perpetrators attack on the environment as a whole or some of its integral parts (e.g., water, air, etc.). In accordance with international legal regulations, this area also includes threats or damage to the environment by a secondary effect of another unlawful activity, e.g., when unlawfully handling nuclear or radioactive materials.

Year	Reported environmental criminal offences	Commenced criminal prosecution	Cleared up (a charge brought)	Percentage (Cleared up / Commenced)
2016	2,482	1,573	982	62.43 %
2017	2,485	1,570	968	61.66%
2018	2,478	1,429	829	58.01%
2019	3,294	1,589	887	55.82%
Total 2016 - 2019	10,739	6,163	3,666	59.48%

In the monitored period 2016 to 2019, out of the total number of 6,163 commenced criminal prosecutions for environmental crime, there were 714[43] cases of conviction (11.59 %), in 53 cases, the penalty of forfeiture of a thing was imposed, in four cases, the forfeiture of property, and in seven cases, the protective measure of confiscation of a thing was imposed.

The damage caused by environmental crime amounts to EUR 44,380,000.00, which is a share of 1.62 % of the total damage. The highest damage was caused in 2016 (EUR 19,770,000.00), and the lowest in 2018 (EUR 5,787,000.00).

[42] Articles 298, 299 Illicit manufacturing and possession of nuclear materials, radioactive substances, hazardous chemicals and hazardous biological agents and toxins, Article 299a Unauthorised construction, Articles 300, 301 Endangering and damaging the environment, Article 302 Unauthorised handling of waste, Article 302a Unauthorised discharge of pollutants, Articles 303, 304 Breach of water and air protection regulations, Article 304a Unauthorised production and handling of ozone-depleting substances, Article 305 Breach of plant and animal species protection regulations, Article 306 Breach of trees and shrubbery protection regulations, Articles 307, 308 Spreading on a contagious disease of animals and plants, Article 309 Escape of genetically modified organisms, Article 310 Poaching, Articles 168, 169 Endangering health due to decayed foodstuffs and other items, Article 212 Theft (only in relation to timber pursuant to Sect.1 (e), Article 378 Inflicting cruelty to animals, Article 378a Breaching the duty of care of animals

[43] The number does not include the number of convictions for Article 212 (1) (e) of the Criminal Code.

The Police Force gradually penetrated into the aspect of this criminal activity; the focus on organised forms of environmental crime allowed detecting various forms and ways of its commission; with the original general approach, they remained hidden.

In the period from 2016 to 2019, there was a certain period of stagnation at the beginning of it, which was caused by reaching a limit of expert capacities of the organisational structure of the Police Force existing at that time and intended for detection and investigation of this type of criminal activity. In 2019, the first step was taken in the gradual change of fight against environmental crime; it was the support of specialisation of policemen in detecting and investigating it by creating first regional departments focused in particular on the detection of more serious forms of environmental crime.

This change started bringing results in the second half of 2019; logically, at first it was seen in an increasing number of detected criminal offences, however, at the same time, another positive fact appeared – the share of detected cases of organised and serious environmental crime increased. The detected cases of organised crime including the cases with an international element proved the importance of specialisation of policemen because extensive economic aspects of this criminal activity including various forms of ML were confirmed.

The continuous analysis of security situation in the area of environmental crime identified several forms of obtaining proceeds from this type of criminal activity and various ways of legalisation.

In main three identified areas of environmental crime (wastes, endangered species of wild fauna and flora, and timber), where various relations to ML were revealed, it should be noted that there is no completely identical model of obtaining and placing proceeds of this criminal activity because very specific and often even professional activities are concerned.

In the area of criminal activity concerning wastes, most frequently it is unlawful obtaining of financial resources by "saving" finances for legal disposal or deposition of waste in such a way that it is illicitly deposited at a place, which is not intended for it; here, international forms of commission of criminal activity are often concerned as in Eastern and Central Europe, the costs of waste storage and disposal are much lower than in Western Europe. Another method is to forge waste quantities or types, in particular through various documents, which reduces "official" costs of its disposal. Disposal of waste into legal landfills beyond the limits of issued permits is also an important method. In such activities, financial resources are "saved" in millions of Euros. The majority of these activities are accompanied by a certain rate of corruption at various State supervision entities, in particular at regional level. The first cases in the territory of the SR showed that this criminal activity takes place in particular internationally, where perpetrators create various complicated chains of companies which trade in or transport wastes. Establishment of such business relationships internationally complicates strongly the activities of the police, and without police specialists for this area, it is not possible to reveal the real scope of this activity.

Proceeds of international organised environmental crime are mostly placed abroad, including non-EU countries because financial operations (payments) also mostly take place outside the territory of the SR.

Within this area, since 2017, an investigation of a legal person and natural persons has been conducted; they had illicitly disposed waste worth more than EUR 6 mil. into an already closed landfill; all the persons charged in this case are permanently propertyless, however, they dispose of expensive real estate and motor vehicles for personal needs. The investigation has shown that waste was transported to the landfill both from Slovakia and from abroad; according to the seized documentation, the waste should have been placed at completely different places or should have been disposed of. The financial resources obtained by this criminal activity are placed abroad and the police cooperate with foreign partners in this case.

In the area of trade in endangered species of wild fauna and flora, perpetrators use various methods of activities related to legalisation. Most frequently, it is illicit import of live animals to the territory of the SR, where subsequently, the perpetrators declare these animals are their own captive animals they reared, and sell them legalised with profit in particular to western Europe.

In one case executed in the monitored period it was found out that one person had had an annual turnover from the sale of parrots amounting to about EUR 300,000.00. The perpetrator smuggled eggs of parrots to the EU (USD 500.00/1 piece), reared them and declared as their own breeding, and subsequently sold them all around the world (EUR 5,000.00 – 7,000.00/ 1 piece).

Other methods include forgery of documentary proofs of origin of fauna and flora, use of the documents of perished animals for new animals smuggled, etc. The obtained financial resources are subsequently reported as high costs of care of animals and operation of rearing facilities or the purchase of veterinary medicines. In fact, the obtained financial resources are mostly invested in purchase of additional animals or used to corrupt supervisory authorities or to purchase real estate for further development of the activity. It appears that this area will require attention because it is not a traditional business activity supervised by competent state authorities; according to Interpol, the financial resources circulating in this "trade" put it almost to the level of trafficking in drugs and human beings.

The last special area related to legalisation is illegal logging and trade in timber. Here, it was found out that illegal logging takes place in the territory of the SR, which is reported, for example, as "removal of calamities" after a wind or pests, logging also exceeds the issued permits, and data on the quality and quantity of timber produced is forged. All these activities are performed with the intention to minimise costs of timber production and mainly to fictitiously reduce the real value of timber, which is then traded. Perpetrators wilfully manipulate timber quality and quantity depending on whether the objective is to obtain financial resources from VAT or another method of obtaining money from the difference. The obtained financial resources are transferred through many companies, which "fictitiously" trade in this commodity, sometimes also for a longer time, and the objective is to complicate the control activities of state authorities. In the previous years, this activity has been carried out internationally; timber has been traded among all countries of Central and Eastern Europe and often, no timber is really imported or exported and these are only "fictitious" business activities. This is possible in particular due to an insufficient system of physical controls of these transactions.

In general, the following can be stated for environmental crime:

- with respect to the specifics of the "goods" in this criminal activity, their quantity and quality are widely manipulated because expertise is needed to determine them correctly,
- there are huge differences in the prices of "goods and services" in this area – both within the EU and outside it,
- perpetrators have certain expertise and abilities and often create relatively closed communities and markets with "specific" goods and services,
- supervisory entities do not have sufficient capacities for efficient control,
- there are no efficient international control mechanisms for selected types of "goods and services" in this area.

Information obtained on the methods of legalisation of proceeds in this area:

- the obtained financial resources are placed in particular abroad or are invested as expenditures within business activities in the purchase of real estate, goods and technology,
- most cases include an international aspect – i.e., there are extensive and numerous (often fictitious) business operations among entities from several countries, where often the quantity and quality of "goods" change, and in the end, it is not obvious where the profit from the transaction is,
- entities, which do not keep mandatory documentation or lose it or destroy, are usually included in the chains of such entities, which thwarts the tracking of movements of money and goods.
-

2.10.2. Forecast of ML threat development in environmental crime

Taking into account the unfavourable development in the area of waste management, we expect extensive development of criminal activities in this area, with the expansion of the described practices, such as forgery of documents on waste quantities and types, forgery of documents on legal disposal of waste, and concealing of waste dumping or releasing into the environment with the objective to obtain financial resources by "saving" costs of its legal disposal.

Environmental crime will also be indirectly supported by the public pressure as a consequence of rising costs of legal waste disposal. More extensive corruption in the affected areas can be expected, and a significant quantity of activities will move to the virtual space – in particular communication, use of virtual currencies and guarantee of anonymity.

In the area of trade in timber, further development of the above illicit activities will continue, in particular the falsification of timber quantity and quality with subsequent trading in the territory of several countries. At the same time, the efforts to produce timber as quickly as possible will be on the rise because of the decreasing reserves and improving control mechanisms and public pressure on the protection of forests.

We do not expect any increase compared to the current state in trade in endangered species of wild fauna and flora.

3. IDENTIFICATION OF SPECIFIC ML THREATS BASED ON THE ANALYSIS OF INVESTIGATED, PROSECUTED AND FINALLY CONVICTED CASES OF LEGALISATION OF PROCEEDS OF CRIME

3.1. PROBLEM OF IDENTIFICATION OF PROCEEDS OF CRIME IN THE CONTEXT OF IDENTIFICATION OF ML THREATS

The overall level of money laundering threat in the conditions of the SR is medium-high in comparison with the neighbouring States. It results from the comparison of estimated scope of their illegal economies expressed as a percentage of GDP (illegal economy includes an estimated financial volume of criminal activity generating illegal income, including money laundering).

According to a publication of the International Monetary Fund,[44] the estimated scope of non-observed economy in the SR is 15.6% of GDP, of it illegal about 0.5% of GDP. The estimated scope of illegal economy in the Czech Republic is 0.4% of GDP, in Hungary 0.8% of GDP, in Poland 0.9% of GDP, in Austria 0.2% of GDP and in Slovenia 0.3% of GDP.

In monetary terms, the scope of illegal economy of the SR in the volume of 0.5% of GDP would represent in 2018 about EUR 450 mil. and in 2019 approximately EUR 470 mil. According to the Annual Reports on the activity of the PF, solely criminal offences of economic nature in 2018 caused a total damage of EUR 284 mil. and in 2019 of EUR 420 mil. **The comparison of the above statistics shows that the scope of unrecorded and in criminal prosecution non-penalised proceeds of crime is only slightly higher.**

Within the activity of law enforcement authorities and courts in the SR, there is no statistical data which would quantify the value of generated proceeds of crime with a sufficient informative capability. One of the reasons is that the determination of composition and amount of proceeds of crime is a qualified process which is part of the taking of evidence in a particular criminal prosecution.[45] In terms of system, it is qualified data which can be de facto finally specified only at the end of the whole criminal proceedings. Such data is not gathered systematically.

However, in the SR, systematically gathered data on the amount of damage caused is available[46] for individual criminal offences. This criterion in the given context provides a view

[44]Shadow Economies Around the World: What Did We Learn Over the Last 20 Years?

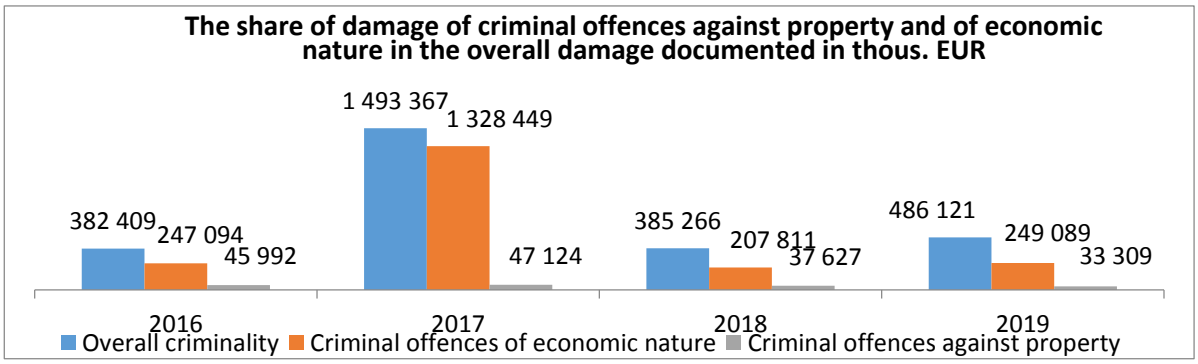
[45] Another problem is that the seizure of proceeds contains its natural stages, which are not distinguished in statistics (e.g., an order for the seizure of financial resources is issued for a certain amount, in fact, a different amount is seized, which can even increase during the seizure). Moreover, the assets acquired legally and illegally naturally mix; plus, other circumstances resulting from the mentioned process.

[46] Article 124 of the Criminal Code

(1) For the purposes of this Act, damage shall mean harm to property or actual loss of assets or prejudice to the rights of the injured party or other harm, which has a causal relationship with the criminal offence irrespective of whether the harm has been caused to a thing or to the rights. **For the purposes of this Act, damage shall also mean advantage gained in causal relationship with the criminal offence.**

of the gravity of criminality committed, as **damage also means advantage gained in causal relationship with the criminal offence.** In criminal law system in the conditions of the SR, damage is an important qualification factor determining the gravity of criminal offence. In principle, however, it can be stated that **the amount of reported damage is higher than the potential volume of proceeds of crime**.

It can be stated from the above-described conclusions of the analysis of individual types of criminality that like in the previous assessment period, in the assessed period from 2016 to 2019, despite the fact that as regards the number of criminal offences committed, criminal offences against property dominate, **as regards the amount of damage, criminal offences of economic nature definitely dominate with a share of 73.98 %. Tax criminal activity with a share of 25.20 % represents a significant part of criminal offences of economic nature. The criminal offences of economic nature are followed by criminal offences against property with a share of 5.97 %.**



In the monitored period, a total damage caused by criminality amounted to EUR 2,747,163,000.00. The damage was negatively affected in particular by one case of criminal offence of economic nature in 2017, when one specific case of distortion of data in financial and commercial records pursuant to Article 259 of the Criminal Code was detected, with a damage caused amounting to EUR 1,118,675,000.00.

As regards particular criminal offences generating the biggest nominal damage, they include in particular tax and insurance premium evasion, fraud, theft, failure to pay tax and insurance premium, embezzlement. The highest damage was recorded for the criminal offence of distortion of data in financial and commercial records, however, it was affected by one case from 2017, as mentioned above.

(2) Damage within the meaning of paragraph 1 shall also mean the loss of profit to which the injured party, considering the circumstances and their personal situation, would otherwise be entitled or could reasonably expect to obtain.
(3) In case of criminal offences against the environment, damage shall mean the combined environmental harm and property damage; property damage shall also comprise the costs of restoring the environment to its original state. In case of the criminal offence of illegal handling of waste pursuant to Article 302, the scope of the offence shall be determined on the basis of customary price charged at the time and place of the offence for the collection, transport, export, import, recycling, disposal or dumping of waste, and the price charged for the removal of waste from the site that is not designated for dumping.

Criminal offences generating the highest damage	Damage caused in thousands of EUR for 2016 - 2019
Distortion of data in financial and commercial records Article 259	1,127,241*
Tax and insurance premium evasion Article 276	326,951
Fraud Article 221	264,007
Theft Article 212	161,346
Failure to pay tax and insurance premium Article 278	89,758
Failure to pay tax and insurance premium Article 277	71,104
Embezzlement Article 213	46,855
Credit fraud Article 222	32,595
Tax fraud Article 277a	24,375
Damaging the European Communities' financial interests Article 261	16,012
Extortion Article 189	15,059
Subsidy fraud Article 225	12,278
Abuse of power by a public official Article 326	10,412
Unlawful manufacturing and enjoyment of payment means, electronic money or other payment card Article 219	4,604

* the high damage was affected by a single case from 2017

In terms of ML, also environmental crime can be assigned to criminal offence generating damage:

- Unauthorised handling of waste Article 302 with a damage caused of EUR 14,171,000.00,
- Breach of trees and shrubbery protection regulations Article 306 with a damage caused of EUR 16,946,000.00,
- Poaching Article 310 with a damage caused of EUR 586,000.00,
- Theft Article 212 (1) (e) in relation to timber, with a damage caused of EUR 1,174,000.00.

However, as regards ML threat definition, it should be noted that in this case the damage caused by detected criminal activity is concerned, without unreported criminality.

Based on a combination of various facts and in accordance with the World Bank's methodology, the working group also identified **the scope of assumed amount of unrecorded proceeds**.

Criminality	Assumed amount of unrecorded proceeds
Criminal violence	except for carrying concealed weapons and arms trafficking, where the proportion of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for criminal violence is not significant
Criminal offences against morality	except for trafficking in human beings, where the proportion of unrecorded proceeds is higher, the proportion of unrecorded proceeds is not significant for criminal offences against morality
Criminal offences against property	the proportion of unrecorded proceeds is slightly higher
Criminal offences of economic nature	the proportion of unrecorded proceeds is (disproportionally) higher
Corruption crimes	the proportion of unrecorded proceeds is higher
Drug-related crime	the proportion of unrecorded proceeds is substantially higher
Organised crime	the proportion of unrecorded proceeds is substantially higher
Environmental crime	the proportion of unrecorded proceeds is (disproportionally) higher
Cybercrime	the proportion of unrecorded proceeds is substantially higher

The following conclusions result from the analysis of **prosecuted and finally convicted cases** of legalisation of proceeds of crime and related character of identified proceeds:

A great part – more than one half of proceeds of crime are immediately consumed by the perpetrator of the predicate criminal offence, without special elements of legalisation.

Legalisation of proceeds of crime in the prosecuted cases was carried out in particular:

- by transferring to bank accounts and withdrawing money from the accounts,
- by selling the stolen and modified things with a concealed origin of acquisition from criminal activity.

These conclusions are quantitatively determined in particular by the scope of prosecuted criminal activity of legalisation, whose subject was the legalisation of stolen cars. However, the conclusion is objectified by consistent examination of all finally convicted ML cases and by the fact that **except for one significant ML case, virtually all seized assets in the convicted ML criminal cases for the mentioned period were returned to the injured persons from the related predicate criminal offences already during the criminal prosecution.**

One **sophisticated scheme** created for the purposes of legalisation of generated proceeds of crime coming from trafficking in substances with anabolic or other hormonal

effects was detected; the proceeds were invested in purchases of real estate in Slovakia, a part of the funds was transferred to tax havens, and one foreign company from the USA was also involved in the chain. Financial investigation is pending in this case and so far, cash amounting to GBP 21,200.00 and EUR 83,500.00 has been seized; based on Article 95 of the Code of Criminal Procedure, financial resources on 15 bank accounts at inland banks amounting to at least EUR 171,500.00 have been seized, and based on a prosecutor's resolution pursuant to Article 425 (1) of the Code of Criminal Procedure, the whole property of the group organiser and the property of two accused legal persons in the amount of at least EUR 1,413,000.00 have been seized.

In organised crime, the biggest sources of illicit proceeds in particular of criminal groups include criminal offences of economic nature, criminal offences against property, drug-related crime, possibly in concurrence with criminal violence.

The experience in the legal contacts with foreign countries shows that like in the previous assessment period, in 2016 – 2019 too, the majority of illicit proceeds are produced by various types of **frauds committed via computer systems, i.e., cybercrime in connection with criminal offences of economic nature with a cross-border character.** In these cases, for example, payments are elicited via the internet for advertised goods, services or based on various sham reasons – loan, winning, etc., money is transferred from accounts to foreign accounts without the owners' knowledge and other; payments go to accounts abroad. Mostly, it is difficult to clarify the cases in the period of limitation of criminal prosecution of predicate criminal offences.

3.2. Assessment of the scope and character of detected, investigated, criminally prosecuted and finally convicted cases of legalisation of proceeds of crime

The essential signs of the criminal offence of **legalisation of proceeds of crime**[47] include the perpetrator's intention to conceal the existence of income or thing, to cover their origin in a criminal offence, i.e., to perform an activity, as a consequence of which the income or thing would seem to have been obtained in compliance with law. Income or other assets, which come from or are reasonable suspected to have come from criminal activity or participation in criminal activity committed in the territory of the SR or out of our territory, can be concerned.

The objective of the perpetrator is, inter alia, to also thwart their seizure for the purposes of criminal prosecution, their forfeiture or confiscation, i.e., to act in such a way as to prevent criminal legal sanctions relating to these things and any pre-trial proceedings.

[47] The provision of Articles 233, 234 of the Criminal Code – Act No. 300/2005 Coll. as amended, by adopting Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts, the title of Article 233 was changed to "Legalisation of proceeds of crime", and, at the same time, a negligence from of this provision was added in Article 233a.

The basic quantitative indicators of criminal prosecution of legalisation of proceeds of crime are as follows:

The basic overview of quantitative indicators of criminal prosecution of legalisation of proceeds of crime for the assessed period						
legalisation					TOTAL	trend
	2016	2017	2018	2019	2016 - 2019	
Total number of postponed UTs	199	123	71	65	458	↓
Number of UTs postponed by the obliged entity/FIU	194/5	118/5	69/2	62/3	443/15	↓
Forwarding the postponed UTs to LEAs	148	87	44	43	322	↓
Forwarding FIU information with suspicion of ML to LEAs	388	273	159	145	965	↓
Commenced criminal prosecution	130	209	149	66	554	↕
Concluded criminal prosecution of unknown persons	118	110	93	100	421	↕
Concluded criminal prosecution of known persons of which:	81	75	36	53	245	↕
Indicted people	39	58	20	32	149	↕
Draft Plea Bargain	5	10	0	2	17	↕
Σ	44	68	20	34	166	↕
Interrupted criminal prosecution	105	98	93	8	304	↓
People convicted	17	26	18	13	74	↕

Holding up the proceeds (all obliged entities)		5,565,757	3,062,393	509,659	1,642,993	10,780,802	↕
Seizure of proceeds (only money, €) within pre-trial proceedings – legalisation/ other offences		63/6,078,580/2,416,882	52/3,028,430/17,212,353	52/1,192,072/60,089,430	48/3,449,150/885,144	215/13,748,520/80,603,810	↑
		252.00%	17.59%	1.98%	389.67%	17.06%	
Seizure total		8,495,462	20,240,783	61,281,502	4,334,294	94,352,330	↑
Asset-related decisions ML/other	Article 58	4/15	6/23	0/23	1/18	11/79	↑
	Article 60	0/821	0/855	1/863	3/560	4/3099	
	Article 83	0/51	0/63	0/71	1/17	1/202	
	Article 56	1/454	0/496	0/596	1/618	2/2137	↑
Really confiscated proceeds in € based on asset-related decisions in criminal prosecution		71,835.88	76,197.82	1,957,672.11	1,094,999.05	3,201,004.86	↑

3.2.1. Detection – identification of cases of legalisation

The Financial Intelligence Unit of the PPF (hereinafter the "FIU SR") is a central national unit in the area of prevention and detection of legalisation of proceeds of crime and terrorist financing. The FIU SR is part of the global network of FIUs, whose task is to apply the international standards of the Financial Action Task Force (hereinafter the "FATF") in combating money laundering and terrorist financing.

Based on the act on the protection against money laundering[48] (hereinafter the "AML Act"), the FIU SR is preferably focused on receiving, registering, analysing, evaluating and processing reports on unusual transactions (hereinafter the "UTs") from banks, various financial institutions, which are not banks, and non-financial institutions.

[48] Act No. 297/2008 Coll. on the protection against money laundering and terrorist financing and on the amendment to certain acts as amended

3.2.1.1. Suspending UTs based on the AML Act

The suspension of an UT pursuant to Article 16 of the AML Act by an obliged entity is an important legal act within the efficient fight against legalisation of proceeds of crime, which is used in the event of a danger that UT execution may frustrate or substantially hinder the seizure of proceeds of crime or resources intended for terrorist financing. Since 1 January 2016, the time-limits for UT suspension carried out by an obliged entity have been 120 hours, and if the case is forwarded to a competent law enforcement authority by the FIU SR, the period is extended by additional 72 hours.

For the monitored period from 2016 to 2019, the FIU SR suspended in accordance with the provision of Article 16 of the AML Act 458 transaction in a total amount of EUR 24,483,362.27.

If during verification of the suspended UT, the suspicion of commission of a criminal offence was confirmed, information was forwarded to law enforcement authorities; in the monitored period, 251 UTRs were forwarded to law enforcement authorities in connection with the suspicion of legalisation of proceeds of crime.

The total suspended amount from the UTRs forwarded was EUR 10,602,390.49, which represents a share of 43.30 % of the suspended financial resources.

Year	Number of suspended UTs in compliance with Article 16 of the AML Act	The value of UTs suspended by obliged entities and FIU SR	Number of suspended UTs and forwarded to LEAs in connection with legalisation	Total value of suspended UTs in connection with legalisation
2016	199	28,039,385.00	112	5,565,271.00
2017	123	9,895,434.00	77	2,943,550.49
2018	71	4,017,793.52	29	494,630.00
2019	65	7,766,749.75	33	1,598,939.00
2016-2019	458	24,483,362.27	251	10,602,390.49

In the monitored period from 2016 to 2019, the FIU SR forwarded to law enforcement authorities (Criminal Office Police of DH PF or Criminal Office Police of RH PF) 965 cases in connection with the suspicion of legalisation of proceeds of crime (of which 251 suspended UTs – a share of 26.01 %). Based on the delivered feedbacks concerning the forwarded information it was found out that PF investigators commenced criminal prosecution pursuant to Article 199 of the Code of Criminal Procedure in 310 cases, in 75 cases, a charge was brought pursuant to Article 206 of the Code of Criminal Procedure, 173 persons were charged and 61 persons were convicted.

In the cases when the FIU SR obtained information which could be used within tax proceedings, the information was forwarded to the Financial Directorate of the SR. For the period from 2016 – 2019, in total 4,308 pieces of information were forwarded; based on them,

the Financial Administration commenced tax audits in 1,928 cases. In performing the tax audits, the Financial Administration employees verified whether any illicit tax evasion or tax fraud had occurred.

The lower number of commenced criminal prosecutions and of accused, indicted and convicted persons results from the fact that in verifying the cases, it was confirmed that the financial resources were legal (e.g., a gift or loan, etc.), some cases did not fulfil the criteria of a criminal offence of legalisation, or if a case included an international element, information was forwarded abroad, where the proceedings took place. However, it should also be noted that some of the forwarded information is still in the process of investigation or have not been concluded yet.

In the first NRA as well as in the period from 2016 to 2019, the forwarded information concerned in particular **the cases of CEO frauds, internet frauds and sham transfers with a link abroad**. As regards CEO frauds, there has been a **significant decrease** since 2019 caused by the cautiousness of banks' customers provided for by increased edification by banks as well as by repressive units of individual States in the area of such criminal activity as it was a criminal activity with an international element.

Compared to the previous assessment period, in 2019, new cases were recorded concerning transactions related to "romance scam" frauds. These were frauds with the objective to elicit cash by using emotional insisting, when perpetrators contacted the injured persons via an e-mail, social networks or sites offering online dating. These types of cases are not directly related to ML/FT, however, the FIU SR forwarded such cases to LEAs in order to prevent such criminal activity and to reveal its perpetrators.

In the detected cases, the FIU SR also cooperated with foreign FIUs of affected States. However, in most cases no criminal proceedings took place because foreign banks, in order to avoid the risk of damaging the reputation in connection with criminal proceedings, indemnified the injured customers.

3.2.1.2. Exchanging information with foreign FIUs

A fast and efficient exchange of information at international level is a precondition for comprehensive and efficient examination of cases of money laundering or terrorist financing.

The FIU SR exchanges intelligence information using a secured encrypted electronic communication network - ESW (Egmont Secure Web) created for that purpose within the international organisation Egmont Group associating units from around the world. Information concerning the detection and documenting of ML/FT cases is also exchanged among the financial intelligence units of EU Member States using the FIU.NET encrypted network.

Information exchanged is exclusively of intelligence character. If such information is to be used in criminal proceedings or any other official proceedings as evidence, it is necessary to apply for such information via the international legal assistance provided for by the General Prosecutor's Office of the SR.

In the assessed period, the FIU SR cooperated in exchanging information in particular with the partner FIUs from the Czech Republic, Hungary, Germany, Austria, Poland, Italy, and the Netherlands. There was more information sent by the FIU SR to foreign States (2,409 pieces of information) than information from abroad to the SR (2,007 pieces of information).

As regards the share of foreign entities (natural persons and legal persons) in the reports sent by Slovak obliged entities in accordance with the AML Act, **mostly entities from Hungary, the Czech Republic, Italy, Poland and Romania were included,** like in the previous assessment period; they were also the most frequently reported entities to LEAs in connection with the suspicion of legalisation of proceeds of crime.

If the FIU SR evaluated the obtained information as information necessary for foreign intelligence units, for the purpose of prevention and elimination of legalisation of proceeds of crime and terrorist financing, it was forwarded directly to a foreign FIU of a particular State for further use.

3.2.2. Basic facts found on the basis of the World Bank's methodology

Based on the 1B module, particular cases of criminal prosecution of legalisation of proceeds of crime were manually assessed. The police proceeded in this way in all cases, in which a resolution pursuant to Article 199 (1) of the Criminal Code (commencement of criminal prosecution) was issued in the respective calendar year, the Prosecutor's Office and the Ministry of Justice – based on an analysis of final court decisions within the period. Moreover, a comprehensive overview of convicted criminal cases was prepared, which contains the most important quantitative and qualitative data and is a significant source of knowledge in the above area.

Law enforcement authorities carry out investigations of ML cases in criminal proceedings **based on their own knowledge from the criminal complaints filed by injured persons, based on legal assistance, etc**. to a disproportionally greater extent compared to the cases when **the FIU SR** initiates investigations.

In the monitored period from 2016 to 2019, police authorities assessed 336 ML cases (116 cases on the basis of information forwarded from the FIU SR), which is only 0.48 % of the total number of all committed criminal offences – 69,635. Out of the total number of assessed ML cases, 64 were cleared up, which means a clear-up rate of 19.05 %[49]. The low percentage of clear-up rate is caused by the fact that out of 336 ML cases, 87 cases are at a stage of investigation, and in as many as 185 cases, criminal prosecution was suspended pursuant to

[49] The cases in which a bill of indictment was filed or the investigation was ended in a way reported as cleared up although no particular person was accused (e.g., due to the inadmissibility of criminal prosecution, absence of a witness, transfer of criminal prosecution abroad) are reported as cleared up in the registration statistical system of criminality of the PF.

Article 228/1 of the Code of Criminal Procedure or terminated pursuant to Article 215/1a of the Code of Criminal Procedure [50].

These were mainly wilful criminal offences and so-called main ML cases, whose priority goal was to possess, use or legalise the things and income from criminal activity. The cases of crime of omission held a much lower share, where the criminal offence of legalisation of proceeds of crime pursuant to Article 234 of the Criminal Code represented only 1.19 % of all ML cases. The number of ML cases did not change much during the monitored period from 2016 to 2018 (86 – 110 cases), only in 2019, there was a significant change, when the number of ML cases recorded was by almost one half lower than in the previous year (50 cases).

The criminal offence of legalisation of proceeds of crime included in particular:

transfers of financial resources from accounts kept abroad; legalisation was usually deduced only from the fact that it was a suspicious payment based on an additional notice from the sending foreign bank, and in general, it was difficult to determine the real identity of the person who had made the payment in the foreign country or established the account in our country. Investigation is also complicated and protracted by the acts of active legal assistance, often to several States, sometimes out of the EU.

Serious ways of commission of criminally prosecuted legalisation of proceeds of crime are interconnected with the most serious forms of criminal activity committed in various sophisticated ways, where the detection, taking of evidence and investigation of predicate criminal offences is time-consuming demanding, as regards contents. In such cases, law enforcement authorities have only limited personnel and technical possibilities of proving a predicate criminal offence along with the method of legalisation of proceeds of crime. Primarily, sufficient conditions for the identification of proceeds of crime are not available. In the absence of proactive parallel investigation, it is virtually impossible.

For the period 2016-2019, the Prosecutor's Office, in connection with legalisation (Articles 233, 234)

- has concluded the criminal prosecution
    - of unknown persons in 421 cases
    - of known persons in 245 cases
        - out of it, in 149 cases, it brought an indictment,
        - in 17 cases, it concluded a plea bargain, and
        - in 10 cases, conditionally discontinued the criminal prosecution.

[50] Termination of criminal prosecution pursuant to Article 215 (1) (a) of the Code of Criminal Procedure: The prosecutor shall terminate the criminal prosecution if it is beyond any doubt that the act, on the grounds of which the criminal prosecution is to be instituted, did not occur.
Suspension of criminal prosecution pursuant to Article 228 (1) of the Code of Criminal Procedure: A police officer shall suspend the criminal prosecution if no grounds were established warranting the criminal prosecution against a certain person.

3.2.3. Final decisions

All court decisions of conviction for legalisation of proceeds of crime pursuant to Article 233 and Article 234 of the Criminal Code for the period from 2016 to 2019 were assessed based on the World Bank's methodology.

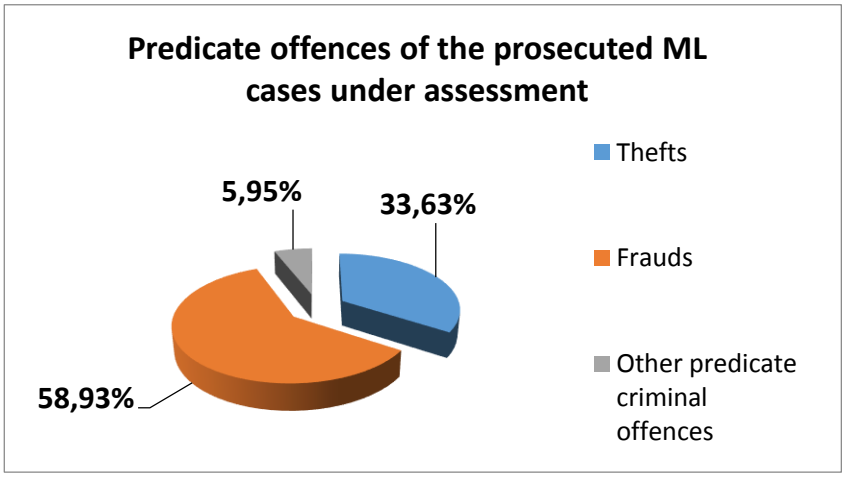
After the statistics of the Analytical Centre of the MJ SR and General Prosecutor's Office of the SR had been cross-checked, 43 final court decisions were assessed for the period 2016-2019.

Based on the assessment of the contents of final judgements for legalisation of proceeds of crime pursuant to Articles 233, 234 it was found out that out of **43 convictions and 65 convicted persons,** 42 convictions and 63 persons were convicted pursuant to Article 233 of the Criminal Code and one conviction and two persons were convicted pursuant to Article 234 of the Criminal Code (in 2017). In all cases, **only natural persons were convicted of ML**. As in the period from 2016 to 2019, a variable development was recorded, despite the adopted measures at the level of the police and Prosecutor's Office, **a positive trend of penalisation of money laundering in the SR cannot be determined.**

Positive tendencies can be seen only at the end of 2019 and in 2020, in the area of commenced criminal prosecutions (charges brought) for some specific types of predicate criminal activity (corruption, environmental crime), which, however, will be subject to a subsequent iteration of NRA.

3.3. Composition of predicate criminal offences in assessing the criminal prosecutions for legalisation of proceeds of crime

The biggest share of the predicate criminal offences of assessed commenced criminally prosecuted ML cases was represented by frauds (58.93 %) followed by thefts (33.63 %). The other predicate criminal offences[51] occurred only marginally with a share of 5.95 %.



As regards fraudulent activities, they included in particular frauds committed abroad with subsequent unauthorised transfers of financial resources, and frauds on the basis of a "false manager's" instruction – CEO frauds were increasingly detected in this group with a share of 12.12 %. In thefts, in particular motor vehicles were of interest for perpetrators (25.30 %).

When compared with the previous round of NRA, it can be stated that the number of detected cases is at a constant level. **The way of commission of ML cases changes** (profiles) from the so far most frequently committed predicate criminal offence (legalisation of motor vehicles often stolen abroad) **to ML cases committed in connection with unauthorised transfer of financial resources via the internet** (internet banking), where the funds come from criminal activity (fraudulent activity or fraudulently elicited payments). The financial resources are often sent to Slovakia from abroad, with the objective to conceal the origin of such acquired financial resources in criminal activity and to thwart their seizure for the purposes of criminal prosecution. The reason for the change may be the fact that perpetrators gradually desist from "simpler" methods of committing ML cases in connection with legalisation of stolen cars, whose proceeds are not so much attractive anymore in proportion to the risk of revelation. Currently, perpetrators try to focus on an unquestionably higher rate of anonymity of the internet and online space, which ensures a considerable decrease in the risk of revelation, with

51 Embezzlement, Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors, Breach of regulations governing state technical measures for labelling goods, Forgery and fraudulent alteration of control technical measures for labelling goods, Illicit production of alcohol, tobacco and tobacco products, Human smuggling, Receiving a bribe, Tax and insurance premium evasion, Establishing, masterminding and supporting a criminal group, Damaging the European Communities' financial interests, Subsidy fraud, Credit fraud, Failure to pay tax and insurance premium

the possibility of a higher profit in fraudulent activities in connection with unauthorised transfers of financial resources through banking institutions or using their services.

In terms of the possible clear-up rate of offences, the international element occurs only to a limited extent. Five detected ML cases also involved persons from organised or transnational groups.

As regards the geographic origin, the proceeds generated in the territory of the SR statistically prevail, like in the previous assessment.

However, this situation did not prove true in assessing finally concluded criminal cases of legalisation of proceeds of crime. Here, criminal cases of legalisation of stolen motor vehicles (almost 19% of finally convicted criminal cases), or associated criminal cases (falsification and fraudulent alteration of motor vehicle identification numbers) continued to dominate. In this type of criminal activity, all types of laundering were identified (self-laundering, autonomous laundering, as well as laundering by a third person). Fraudulent activities and embezzlement represented predicate criminal activity in 9 %. However, here it is important to note that legalisation by a third person or autonomous laundering prevailed. In six cases (4 %), a conviction was achieved, in connection with predicate criminal activity committed in an organised form (autonomous laundering or self-laundering). Counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark was identified as a frequently used instrument for commission of predicate criminal activity or related legalisation.

Overall overview of identified predicate crime, finally concluded ML cases					
	2016	2017	2018	2019	Σ
Article 212	11	9	3	5	28
Article 219				1	1
Article 220	2	4			6
Article 221 (Article 250)	1	4	2	2	9
Article 213 (Article 248)			1		1
Article 237	1				1
Article 326	1				1
Article 172		1			1
Article 356		1			1
Article 352		1		1	2
Article 274			1		1
Article 276				1	1
Article 296	1	2		2	5

Overview of identified predicate crime, finally concluded ML cases AUTONOMOUS LAUNDERING					
	2016	2017	2018	2019	Σ
Article 212	7	1		2	10
Article 220	1				1
Article 221 (Article 250)	1	1		2	4
Article 213 (Article 248)			1		1
Article 326	1				1
Article 276				1	1
Article 296	1	1		1	3

Overview of identified predicate crime, finally concluded ML cases SELF-LAUNDERING					
	2016	2017	2018	2019	Σ
Article 212	1	5	1	2	9
Article 219				1	1
Article 220		3			3
Article 237	1				1
Article 326	1				1
Article 172		1			1
Article 356		1			1
Article 352		1		1	2
Article 276				1	1
Article 296		1		2	3

Overview of identified predicate crime, finally concluded ML cases 3rd party ML					
	2016	2017	2018	2019	Σ
Article 212	4	3	2	2	11
Article 220	2	1			3
Article 221 (Article 250)	1	4	2	1	8
Article 352				1	1
Article 274			1		1
Article 296	1	1		1	3

The above mentioned also affects the conclusions regarding the cross-border dimension of predicate criminal activity:

The analysis of convicted cases shows that the proceeds laundered in the SR were generated in the SR (5x) and 2x the Czech Republic, 1x USA, 1x Cayman Islands and 1x China. The countries which the proceeds were directed to, placed or legalised in (unless they were

place in the SR – at least eight cases) are as follows: 1 x USA, 1x Poland, 1x China, and 1 x United Kingdom.

Thus, based on the logics of criminal proceedings it is objective to expect a change of structure of predicate criminal activity for finally concluded criminal prosecutions when they come to a stage of court proceedings.

3.4. Proceeds in the assessed criminal prosecutions of legalisation of proceeds of crime

In the commenced criminally prosecuted ML cases, the subject of legalisation was property (detected financial resources, things used, income or property in an ML case) in the amount of EUR 193,817,782.82 and CZK 122,375,837.14 (the amount of 1B tables). It should be noted here that it is not a final amount because statistically not in all of the cases, the value of property legalised was properly documented (in particular, for example, for vehicles stolen abroad, legalisation of vehicles coming from criminal offences, etc.). For this reason, the data has only an approximate informative capability.

3.4.1. Seizure of proceeds in the assessed criminal prosecutions of legalisation of proceeds of crime

The comparison of statistical data shows another factor of inefficiency, which weakens a total efficiency of the AML process – a low volume of confiscation of proceeds of crime.

The total value of seized property (financial resources, things, income or property) in these assessed ML cases amounted to EUR 13,748,519.85, CZK 3,117,700.00, USD 6,507.00, PLN 36,510.00 and GBP 21,200.00.

Statistically, only 7.09 %[52] (the value only in EUR) of the nominal volume of the legalised property value identified in criminal prosecution was seized.

However, the above quantitative data need to be interpreted in a broader context because in addition to seizure of financial resources on accounts (or cash), also things were seized as proceeds (in particular within the duty to surrender a thing and by confiscating a thing), or a whole property or particular real estate, which were not valuated and are not recorded in the above statistics. The working group also dealt with the assessment of the content of statistical data of the Police Force in this area, however, it came to a conclusion that it is not possible to specify unambiguously for the reported data whether it was a thing important for proceedings (as evidence) or proceeds of crime or a claim of the injured person. In assessing a value, only estimated data is often entered or no data is entered at all, which would considerably deform the assessment of weight of the data for the above purpose[53].

[52] This is data for criminally prosecuted ML cases Article 199 table Module 1B – Total detected amount of EUR 193,817,782.82 in relation to Total seized amount. However, the data provided does not take into account currencies other than EUR because conversion into EUR is impossible. Other resources in the currencies CZK, USD, PLN, GB were also seized; however, they are not included in the total amount of seized financial resources.
[53] When seizing proceeds, policemen often follow Article 89 of the Code of Criminal Procedure (surrender of a things) and prosecutors Article 95 of the Code of Criminal Procedure (seizure of funds). The legal regulation

A statistical overview of the scope of application of selected seizure methods of the Code of Criminal Procedure in criminal proceedings for all criminal offences and for criminal offences of legalisation of proceeds of crime pursuant to Articles 233, 234 of the Criminal Code provided in the Annual Reports of the FIU SR:

Seizure of proceeds according to the statistical data of the FIU SR*		
		The duty to surrender a thing Article 89 of the Code of Criminal Procedure, Seizure of a thing Article 91
2016	ML cases / all cases	64,900 / 3,574,816
2017	ML cases / all cases	852,787 / 2,352,250
2018	ML cases / all cases	289,330 / 6,246,527
2019	ML cases / all cases	23,850 / 0
Total 2016 - 2019	ML cases / all cases	1,230,867 / 12,173,593

* A statistical overview of the scope of application of selected seizure methods of the

Code of Criminal Procedure in criminal proceedings for all criminal offences and for criminal offences of legalisation of proceeds of crime pursuant to Articles 233, 234 of the Criminal Code prepared by the FIU SR from data sent by unites of the PF of the MI SR, from the FACO, criminal department of the GPO SR, Special Prosecution Office of the GPO SR and MJ SR in accordance with Article 27 (3) of the AML Act.

Real seizure of money according to the analysis of the GPO SR to NRA in EUR currency + other currencies		
	ML cases	Other criminal offences
2016	6,078,580.13	2,416,882.14 + CZK 292,947.11
2017	3,028,717.31	17,212,353.38 + CZK 2,000.00
2018	1,192,072.10	60,089,429.67 + BTCN 161.90957883
2019	53,449,150.31	885,144.36
2016-2019	13,748,519.85	80,603,809.55+ CZK 294,947.11+ BTCN 161.90957883

effective till 31 December 2015 virtually did not allow the prosecutors to return the seized financial resources to the injured persons if ownership of the financial resources was ascertained and proven, and another person also exercised the right to them. The defect was resolved only by an amendment to the Code of Criminal Procedure, by adding the provisions of Article 95a and Article 95b of the Code of Criminal Procedure.

The whole Prosecutor's Office SEIZURE OF PROCEEDS (MONEY) Basic overview NUMBER OF REALLY EXECUTED ORDERS and REALLY SEIZED VALUE						
		2016	2017	2018	2019	2016 - 2019
TOTAL District Prosecutor's Office	ML	30 3,097,476.58	16 2,743,466.74	14 1,108,110.01	10 858,750.76	70 7,807,804.09
	Other	19 2,070,382.42 + CZK 292,947.11	23 425,255.54	23 1,459,502.75 + BTCN 161.90957883	28 833,640.04	93 4,788,780.75 + CZK 292,947.11 + BTCN 161.90957883
	Σ	49 5,167,859 + CZK 292,947.11	39 3,168,722.28	37 2,567,612.76 + BTCN 161.90957883	38 1,692,390.80	163 12,596,584.84 + CZK 292,947.11 + BTCN 161.90957883
TOTAL Regional Prosecutor's Office	ML	5 2,981,103.55	5 285,250.57	1 73,962.09	7 2,590,399.55	18 5,930,715.76
	Other	6 177,499.72	5 250,871.84 + CZK 2,000	3 41,145.92	3 51,504.32	17 521,021.80 + CZK 2,000
	Σ	11 3,158,603.27	10 536,122.41 + CZK 2,000	4 115,108.01	10 2,641,903.87	35 6,451,737.56 + CZK 2,000
TOTAL SPO	ML	0	0	1 10,000	-	1 10,000.00
	Other	3 169,000	3 16,536,226	10 58,588,781	-	16 75,294,007.00
	Σ	3 169,000	3 16,536,226	11 58,598,781	-	17 75,304,007
TOTAL	ML	35 6,078,580.13	21 3,028,717.31	16 1,192,072.10	17 3.449.150,31	89 13,748,519.85

for PO	Other	28 2,416,882.14 + CZK 292,947.11	31 17,212,353.38 + CZK 2,000	36 60,089,429.67 + BTCN 161.90957883	31 885,144.36	126 80,603,809.55 + CZK 294,947.11 + BTCN 161.90957883
	Σ	63 8,495,462.27 + CZK 292,947.11	52 20,241,070.69 + CZK 2,000	52 61,281,501.77 + 161.90957883 BTCN	48 4,334,294.67	215 94,352,329.40 + CZK 294,947.11 + BTCN 161.90957883

Further, we provide an overview of the Prosecutor's Office concerning other seized property (immovable and movable assets, other than money on accounts). The added value of this overview is the documented fact that compared to the previous period, the scope and volume of seizure of proceeds in criminal proceedings acquires signs of systematic understanding, a mechanism based on adopted measures in the area of financial investigation. In substance, these are very important facts as in the case of seized real estate, these are significant forms of placing proceeds of crime, and perpetrators of predicate criminal offences are strongly affected (e.g., the seizure of the building of a *business centre* – Technopol – by a prosecutor of the SPO GPO SR, or the below example of seizure of property in a tax criminal case by a prosecutor of the Regional Prosecutor's Office Žilina). Record-keeping and reporting the value is a problem because it would require an expert opinion.

However, after eliminating the vulnerability elements in the area of seized property management (as a consequence of Act No. 312/2020 Coll.), there is a real justified assumption for the intensification of the prosecutors' activities in the area of property seizure based on the results of intensified performance of systematic proactive financial investigation of policemen.

	OVERVIEW OF OTHER SEIZED PROPERTY Movable and immovable assets – OTHER THAN MONEY ON ACCOUNTS The whole Prosecutor's Office -				
	Movable assets		Immovable assets		TOTAL
	description	about €	description	about €	
2016	Regional Prosecutor's Office	329.795,72			
	District Prosecutor's Office	533.745,68 CZK 3,135.00 USD 1			
	SPO	19,000.00		150,000.00	
	Total	882,541.40 CZK 3,135.00 USD 1	Total	150,000.00	1,032,541.40 CZK 3,135.00 USD 1

2017	Regional Prosecutor's Office	877,405.39		357,000.00	
	District Prosecutor's Office	275,861.99 HUF 8,000.00 CZK 74,000.00			
	SPO	0		1,500,000.00	
	Total	1,153,267.38 HUF 8,000.00 CZK 74,000.00	Total	1,857,000.00	3,010,267.38 HUF 8,000.00 CZK 74,000.00
2018	Regional Prosecutor's Office	472,947.80		374,000.00	
	District Prosecutor's Office	396,518.41 HUF 4,000.00			
	SPO	21,688,781.00		37,000,000.00	
	Total	22,558,247.21 HUF 4,000.00	Total	37,374,000.00	59,932,247.21 HUF 4,000.00
2019	Regional Prosecutor's Office	394,947.30 + USD 570.00 PLN 1,480.00		15,676.00 + other real estate, value undetermined	410,623.30 + USD 570.00 PLN 1,480.00
	District Prosecutor's Office	158,590.00		1,600,000.00	1,758,590.00
	SPO	500.00		2,630,000.00	2,630,500.00
	Total	554,037.30 + USD 570.00 PLN 1,480.00	Total	4,245,676.00	4,799,713.30 + USD 570.00 PLN 1,480.00
TOTAL		€25,148,093.29 + CZK 77,135.00 + USD 571.00 + HUF 12,000.00 + PLN 1,480.00		€43,626,676.00 + other real estate, value undetermined	68,774,769.29 + CZK 77,135.00 + USD 571.00 + HUF 12,000.00 + PLN 1,480.00

Kv 53/19/5500 – Regional Prosecutor's Office Žilina
Investigation case No.: KRP-72/2-VYS-ZA-2019 – RH PF Žilina
2 accused persons - A.B. and J.B.
legal qualification: Article 20, Article 276/1/4 OZ – both persons

Article 233 / 1ab / 4a OZ - only A.B.

Factual basis:

Tax evasions – at least for two years, in 2017 and 2018, both A.B. and J. B. organised import of great quantities of car tyres from Poland and sold them to end customers in Slovakia through two e-shops operated by them. Formally, the trade was provided for by two limited liability companies with A.B. as real owner of both companies; formally, they were managed by dummies – homeless people of Hungarian and Polish origin. These two companies never fulfilled value added tax resulting from running a business in Slovakia (sale to end customers); import of tyres from the EU is not subject to VAT. Although they formally reported VAT in the form for an invoice to end customers, it was never reported to tax authorities and deducted from the grow income of the company. This scheme allowed the two electronic shops to be the cheapest suppliers around, and thanks to tax evasions, their business could be extended to a large scope. Tax evasion determined at the beginning of criminal prosecution - €601,782.83.

Legalisation signs – in the period from 20 April 2018 to 16 May 2018, A.B. transferred, within 16 transactions, a total amount of €206.105.00 from the bank account held by one of the companies involved in the scheme of tax entities to their private account and then transferred the amount to various bank accounts registered for their family members – probably with the intention to conceal the cash flow, which would prevent the activity of authorities in the area of monitoring.

There is a strong suspicion that the proceeds of "business" of the company of A.B. were invested in real estate – it is obvious that the scope of ML will grow with the progress of investigation.

The following was seized in cooperation with FACO, Real Estate Register and Commercial Register:

4 bank accounts seized based on Article 95 of the Code of Criminal Procedure – the amounts seized so far:

1) €3,428.06
2) €131.95
3) €79,577.63
4) €129,374.54

Cash seized during home searches:

€87,473.30
USD 570.00
PLN 3,660.00

One newly constructed flat seized by prosecutor's decision pursuant to Article 461/2 of the Civil Procedure Act dated 29 November 2019 – a value of €15,676.00 (costs of construction, not the market value)

The flat was formally registered as belonging to the father of A.B. but the construction was financed by A.B. from proceeds of crime – seizure of additional real estate is expected because registration of construction and ownership by family members of A. B. is expected.

It results from the analysis of cases that the greatest obstacle in seizing proceeds is the absence of proactive financial investigation.

Only Article 119 (1) (f) of the Code of Criminal Procedure corresponded to this requirement in technical terms in the assessed period. The National Unit of Financial Police of the PPF, the department of property verification (till 31 January 2017, it was part of the FIU SR) should have been a cooperating professional authority of the police. However, in the assessed period, LEAs were not able to involve these authorities to a greater extent and systematically in the process of detection of proceeds of crime. The above processes contain a necessary requirement of multi-sectoral specialisation. Moreover, without efficient seizure of property in initial phases of criminal prosecution, basic conditions for confiscation of proceeds of crime will not be created.

In 4Q 2019, Order of the President of the PF dated 3 October 2019 No. PPZ-KP-OVYS-2019/051760-001 as amended was adopted; it specified the job description for newly established two financial investigation specialists at each other District Unit of the Criminal Police Department of the TH PF, i.e., 16 specialists for the territory of the SR. These specialists preferably prepare the property profile of a person of interest by screening and through requests sent to affected entities. The average preparation of a simple property profile lasts about 2-3 months. Samples of filings and statistics for property profiles and for the reporting of value and character of seized proceeds of crime were prepared, with effect of reporting from 1 January 2020. The above statistical instruments were also forwarded to NAKA and Inspection Service Office for the purpose of uniform procedure and statistical reporting. **The comprehensive indicators of efficiency of financial investigation will be processed in the National Risk Assessment for the next period**. This task also results from the approved Action Plan for fight against ML/FT.

Outside the framework of the assessed period in 4Q 2020, there was a considerable legislative strengthening of financial investigation instruments and seized assets management by adopting Act No. 312/2020 Coll. with effect from 1 January 2021, which, inter alia (establishment of an Office for Seized Asset Management, change of criminal material law in the facts of the criminal offence of legalisation of proceeds of crime), introduced new procedures, such as seizure of real estate, seizure of a business interest, virtual currencies or any other values in the procedure after the commencement of criminal prosecution. The purpose of criminal prosecution was also expanded, which expressis verbis also includes confiscation of proceeds of crime. The above act also facilitated the use of financial investigation outputs as evidence in criminal proceedings, which are usually executed through the procedure according to a special act, in accordance with a newly formulated provision of Article 119 (2) of the Code of Criminal Procedure. The real impacts of the new legal framework will be evaluated in the next iteration of the NRA.

Outside the framework of the assessed period, it should be pointed out that by the end of 2021, a specialised department for financial investigation with national competence will be established in the territory of the SR, in total 172 policemen will carry out this activity. This fact also represents the fulfilment of the Government Manifesto.

Proceeds of crime in a tax criminal case conducted at the Criminal Police Department of the RH PF ZA in a total volume of about EUR 80,000.00 in cash, about EUR 300,000.00 on bank accounts, and three real properties (a flat and two lands) in the total value of about EUR 350,000.00 were seized in 4Q 2019 thanks to excellent cooperation among the Criminal Police Department of the RH PF ZA, Regional Prosecutor's Office ZA and FACO.

3.4.2. Withdrawal of proceeds of crime and the character of sanctions in the assessed criminal prosecutions of legalisation of proceeds of crime

The analysed court decisions for the years 2016 to 2019 in connection with **final withdrawal of proceeds** show that **the penalty of forfeiture of property** pursuant to Article 58 of the Criminal Code was imposed 11 times, **the penalty of forfeiture of a thing** pursuant to Article 60 of the Criminal Code 4 times and **the protective measure of confiscation of a thing** pursuant to Article 83 of the Criminal Code once. Compared to the 1st round of NRA, when withdrawal of proceeds by direct instruments in the cases of money laundering was imposed to a minimum extent, it is a positive development. However, in terms of efficiency, the comparison with confiscations imposed for other criminal offences should be taken into account; in the years 2016 to 2019, in total 79 penalties of forfeiture of property were imposed, 3099 penalties of forfeiture of a thing and 202 protective measures of confiscation of a thing.

A progress also occurred in confiscating **proceeds** of legalisation of proceeds of crime pursuant to Article 60 (1) (c), (d) of the Criminal Code as a thing which the perpetrator acquired through a criminal offence or as a reward for it.

This is, for example, the case "Nephew" from 2019 concerning the transfer of untaxed financial resources from import of lubrication and heating oil and its sale as diesel oil, and the subsequent purchase of real estate and motor vehicles using the illegally obtained resources, when the Special Criminal Court imposed the penalty of forfeiture of a thing pursuant to Article 60 (1) (c) of the Criminal Code (an amount of **EUR 19,560**), the penalty of forfeiture of a thing pursuant to Article 60 (1) (c) of the Criminal Code (an amount of **EUR 2,845**) and the penalty of forfeiture of a thing pursuant to Article 60 (1) (d) of the Criminal Code (a single-family house, industrial building, tourist hostel, industrial premises, hotel, 4 motor vehicles – **in a total value of EUR 1,145,450**), **thus also confiscating the proceeds of this criminal activity and real estate along with vehicles obtained from these proceeds**. At the same time, this judgement also imposed the **confiscation of a thing** pursuant to Article 83 (1) (a) of the Criminal Code – cash amounting to **EUR 1,130**, cash amounting to **EUR 9,264**, trucks with tractors and semi-trailers, as well as mineral oil belonging to legal persons, which could not be prosecuted.

Despite the above-mentioned, there were also cases, when with imposed penalties of forfeiture of a thing, courts confiscated **only the tool** used for the legalisation of proceeds of crime pursuant to Article 60 (1) (a), (b) of the Criminal Code and not the proceeds.

For example, the penalty of forfeiture of a thing imposed in 2016 in the case of legalisation by dismantling a stolen motor vehicle worth EUR 5,386 for the purpose of its use as spare parts concerned a transmitter with a charging adapter of unspecified value. In the case of money laundering in 2018 through the transportation, sale and possession of stolen footwear worth EUR 180,000 with real proceeds amounting to EUR 12,000 EUR and potential profit of EUR 9,565, the imposed penalty of forfeiture of a thing concerned only one Lenovo notebook of undetermined value. Although the value of confiscated propertied or things is provided in judgements only exceptionally, it is obvious from some decisions that the value of the confiscated thing is disproportional to the obtained proceeds.

Eleven compulsorily imposed penalties of forfeiture of property[54] concerned in four cases a large bank fraud, in two cases a mortgage fraud and establishing, masterminding and supporting a criminal group, in two cases human smuggling and illegal employment of foreigners and in one case, drug-related crime. In two serious cases of money laundering – "*American mortgages"* and "*Nephew",* the penalties of forfeiture of property imposed by the Special Criminal Court were subsequently cancelled by the supreme Court of the SR (for a disproportionate penalty and a fault concerning the principles of imposition of penalties by imposing the penalty of forfeiture of a thing and forfeiture of property concurrently).

The total value of confiscated property pursuant to Article 58, Article 60 and Article 83 of the Criminal Code provided in judgements (the value of property is not provided in most decisions on confiscation) reached **EUR 1,178,249.00**.

Besides confiscations, from the view of proceeds withdrawal also a money penalty can be taken into account; it does not require evidence of acquisition of a thing in an illegal way, however, it was only imposed twice during the monitored period in an amount of EUR 300.00 and EUR 10,000.00, which does not allow considering a money penalty to be an efficient indirect way of withdrawal of proceeds obtained by legalisation of proceeds of crime. Twice in criminal proceedings, the courts also imposed **a duty** on the convicted person **to reimburse damage to the aggrieved persons** in the amount of EUR 1,837.00 and EUR 1,161,787.16. In the third case, the duty to reimburse the damage amounting to EUR 5,000.00 and EUR 728.60 to the injured persons concerned the conviction for theft in Point 2 of the judgement rather than the legalised proceeds. The statistics of results of cases, in which the court referred the injured person with their claim for damages to a civil process, are not available.

In relation to the above mentioned it should be noted that with respect to efficiency, proportionality and dissuasive effect of sanctions, in the examined cases of conviction for legalisation of proceeds of crime, **in particular sentences of imprisonment** (62x, of which 33x suspended) were imposed. They were followed by protective supervision, ban on activity, expulsion or probationary supervision.

54 In 2016 – 4 x, in 2017 – 6 x, in 2018 – 0 x and in 2019 – 1x (2-times cancelled by the Supreme Court of the SR)

Real withdrawal of proceeds of crime based on final property-related court decisions is a problem of efficiency. As the Report from the 5th Round of Evaluation of the SR by Moneyval mentions – the SR is not able to sufficiently prove the real performance in this area.

Formally, the exercise of property-related decisions issued in criminal proceedings falls under the competence of two ministries – Ministry of Justice and Ministry of Interior. In the SR, there is no mechanism of data collection or any methodology.

The following correlation was analysed in this area:

Seizure vs property sanctions vs real deprivation of criminal assets (real recovered) Correlation SEIZURE – PROPERTY SANCTIONS – REAL CONFISCATION OF PROCEEDS									
	SEIZURE			Property sanctions (value not identified)					Real recovery
	Money on bank accounts	Other secured property than Money on bank accounts	TOTAL	Article 58 of the Criminal Code	Article 60 of the Criminal Code	Article 83 of the Criminal Code	Article 56 of Criminal Code	Total	
2016	€8,495,462.27 + CZK 292,947.11	€1,032,541.40 + CZK 3,135.00 + USD 1	€9,528,003.67 + CZK 296,082.11 + USD 1	19	821	51	3129	4020	€71,835.88
2017	€20,241,070.69 + CZK 2,000.00	€3,010,267.38 + HUF 8,000.00 + CZK 74,000.00	€23,251,338.07 + HUF 8,000.00 + CZK 76,000.00	30	855	63	2963	3911	€76,197.82
2018	€61,281,501.77 + BTCN 161.90957883	€59,932,247.21 + HUF 4,000.00	€121,213,748.98 + BTCN 161.90957883 +	23	864	71	2821	3779	€1,957,672.11

			HUF 4,000.00						
2019	€4,334,294.67	€4,799,713.30 + USD 570.00 + PLN 1,480.00	€9,134,007.97 + USD 570.00 + PLN 1,480.00	21	563	18	2658	3260	€1,094,999.05
Total	€94,352,329.40 + CZK 294,947.11 + BTCN 161.90957883	€68,774,769.29 + CZK 77,135.00 + HUF 12,000.00 + USD 571.00 + PLN 1,480.00	€163,127,098.69 + CZK 372,082.11 + HUF 12,000.00 + USD 571.00 + PLN 1,480.00 + BTCN 161.90957883	93	3103	203	11571	14970	€3,201,004.86

A very low efficiency results from the above data – an impact of seizing procedures on property-related sanctions, and in particular an absolutely questionable scope of exercise of property-related decisions of courts based on judgements awarded in criminal prosecution.

An absolutely unsatisfactory ability to withdraw property owned by third persons is a special issue. In this context, there are virtually no examples for generalisation.

In the given context, ML prosecution is no way different from the results of criminal prosecution of (only) predicate criminal offences.

As a consequence of the absence of a systematic approach in this area, it is difficult to provide any substantial related conclusions. Thus, we can only suppose that even if a judgement is awarded for real withdrawal of property – proceeds of crime, it is not withdrawn as a consequence of its non-existence in the legal ownership of the affected person. There is not qualified data in this context, for example, to which extent and at what stage, the affected property is transferred to third persons, etc.

3.5. Characteristics of methods and typology in the assessed criminal prosecutions of legalisation of proceeds of crime

Based on the 1B module of the World Bank's methodology, selected characteristics of ML cases were analysed. Taking into account the terminology and terms used in the manual, which could not be fully applied to the conditions of the SR due to ambiguity and absence of a detailed explanation, a national explanation was applied in some characteristics to ML cases. In assessing ML cases, the way of property legalisation as well as the type of property or thing itself was taken into account.

The following methods of commission and their typology were determined:

1. Transfer of financial resources – the financial resources obtained by fraudulent transfer from another account or phishing, including eliciting the funds fraudulently to a bank account kept by a bank in the SR via e-mail communication were remitted to various accounts and sometimes also subsequently transferred or withdrawn. Taking into account the above-mentioned scheme of criminal activity, these cases involve many entities with a foreign element (the injured person, banking institution, bank account's holder and their statutory body have their registered office/place of residence in various States, often in non-EU States). As the predicate criminal offence is mostly committed abroad and information of the FIU SR or bank often does not provide a sufficient basis to determine the way of commission of the predicate criminal offence, it is necessary to primarily determine its existence and the way of its commission, which cannot be carried out in any way other than through time-consuming requests for legal assistance to foreign countries.
2. Stolen vehicles – legalisation of stolen vehicles by tampering VIN, possession of stolen vehicles or their parts intended for further use or use of stolen vehicles.
3. Consumption of things – consumption or possession and use of various things, or sale of things obtained from criminal activity, most frequently from theft or fraud, in particular consumer electronics was concerned (in this category, two cases are worth mentioning: in the first one, the sale of a "designer drug" was concerned, the Bitcoin cryptocurrency (and other), other drugs, real estate, motor vehicles were purchased for the income, and in the second case, four pictures coming from a theft by breaking in a flat in Vienna were procured, transported to the territory of the Slovak Republic, kept at various places and then sold to another person).
4. Fraud during an act – legalisation or consumption of financial resources fraudulently obtained during various acts, most frequently during a fake sale (issuance of an invoice, payment and failure to supply goods) or by issuing fictitious invoices and entering them into accounting (tax base reduction, tax evasion or ineligible VAT deduction).
5. Illicit sale of real estate - specific ML cases (3), when in the first case, the suspicious person sold the fraudulently acquired real estate, in the second case, the real estate was transferred for EUR 1,000.00 to a related natural person, for the purpose of complete frustration of the possibility to satisfy the creditor's receivable, and in the third case, forged contracts were submitted to the cadastral authority with false signatures in order to illicitly obtain lands to ownership.
6. Failure to fulfil a duty - two ML cases: in the first one, a duty was not fulfilled by an employee of an originality check station, who despite finding out that a vehicle was tampered (tampered VIN), designated the vehicle as original (unaltered), and in the second case, a duty was not

fulfilled by two bank employees who carried out fictitious deposits into and withdrawals from the accounts of a legal person at the request of another person.

3.6. Target country and country of origin

The Slovak Republic is **a target country** in most prosecuted ML cases (in 237 ML cases, which represents a share of 70.53 %). The increase found compared to the previous NRA is interesting; it consists in 43 prosecuted ML cases with transfers of financial resources, where two and more countries were determined as target countries.

It should be noted that in this method, such countries as China, Hong Kong, Malaysia, Israel, Philippines, Taiwan, Benin, South Africa, India, Panama, i.e., non-EU countries were also determined as target countries of ML cases.

In connection with the **country of origin,** the Slovak Republic held the highest share in ML cases (83 cases, meaning a share of 24.70 %), Germany followed (45 cases, meaning a share of 14.47 %), Austria (35 cases, meaning a share of 11.25 %) in particular in connection with thefts of motor vehicles and subsequent legalisation. Like in determining the target country, the number of countries of origin also increased, where two and more countries were determined as countries of origin (49 ML cases).

The following data was found in terms of geographic origin of proceeds in accordance with the methodology in the cases when a bill of indictment was filed:

Breakdown of origin of proceeds Period of collection: 2016-2019 Currency used: €	Number of convictions (things/persons)	Value of seized proceeds of crime (funds + other things)	Value of confiscated proceeds of crime (funds + other things)
Origin of legalised proceeds			
A. generated in the territory of the SR	23/40	€2,560,961.15	6x Article 58 of the Criminal Code 1x Article 56 of the Criminal Code (10,000.00) 3x Article 60 of the Criminal Code (1,074,605.00) 1x Article 83 of the Criminal Code (10,394.05 + in other cases the value was not ascertained) 6x damage compensation (€1,215,226.69) of which 1x the injured person

			referred with their claim (€6,000.00) to civil proceedings 1x damage fully compensated by the perpetrator in pre-trial proceedings
B. generated abroad	18/26	€1,813,638.81+	8x Article 58 of the Criminal Code 1x Article 56 of the Criminal Code (€300.00) 1x Article 60 of the Criminal Code (the value undetermined)
C. generated in the SR and also abroad	-	-	-
D. The country of origin cannot be determined	-	-	-

It is obvious from the above data that statistically, the proceeds generated in the territory of the SR still prevail. However, in terms of quality, a rising trend of detection and subsequent prosecution of money laundering with a cross-border aspect of generating proceeds of crime should be mentioned. This fact is important in particular in the context of an increase in the volume of prosecution of the so-called carousel frauds.

The analysis of convicted ML cases shows the following:

The country, in which the laundered proceeds were generated – 5xSR, 2xCR, 1xUSA, Cayman Islands, China, Mongolia

The country of placing (the country, which the proceeds were directed to, placed in or later legalised in) – 8x SR, 1xUSA, PL, China, UK

The facts concerning active and passive legal assistance are another important element because to a much greater extent they reflect the real involvement of entities from other States in the cases with pre-trial proceedings completed as all necessary circumstances for filing a bill of indictment were the subject of legal assistance.

As regards the active legal assistance in ML cases (the total number of requests 537), most requests for legal assistance were addressed to judicial authorities of Hungary (109 requests, i.e., 20.30 % of the total number of requests), the Czech Republic (80, which means 14.90 %), Germany (79, which means 14.71%) and Italy (31, which means 5.77 %). In this area, UK and Austria are significant (29 requests each, which means 5.40%) and France (16 requests, which means 2.98%).

Table of international legal assistance (only ML cases) The highest numbers of requests sent (active legal assistance) for the period 2016-2019		
Serial No.	Country name	Number of requests
1	Hungary	109
2	Czech Republic	80
3	Germany	79
4	Italian Republic	31
5	UK	29
6	Republic of Austria	29
7	French Republic	16

Passive legal assistance in ML cases (the total number of requests 440) represents the situation when information concerning money laundering in other States is in the territory of the SR (transit or placing of proceeds).

Most requests were sent by judicial authorities of the Czech Republic (132 requests which is 30 % of the total occurrence), Poland (106, which is 24.09 %), Hungary (53, which is 12.05 %), France (22, which is 5 %), and Italy (21, which is 4.77 %).

Table of international legal assistance (only ML cases) The highest numbers of requests received (passive legal assistance) for the period 2016-2019		
Serial No.	Country name	Number of requests
1	Czech Republic	132
2	Republic of Poland	106
3	Hungary	53
4	French Republic	22
5	Italian Republic	21
6	Germany	20
7	Republic of Austria	14

The **scope of seizure executed on the basis of judicial cooperation** in criminal cases is another important factor in assessing the geographic aspect of legalisation threats. **The Slovak judicial authorities actively acted so only exceptionally,** which a significant factor representing **negative connotations in relation to the quality of prosecuted cases.**

Seizure within the international legal assistance for ML is as follows.

No.	Country	The value requested/seized
1	Italian Republic	EUR 5,302,776.53/EUR 258,652.10 USD 246,190.00/ USD 246,190.00
2	The Netherlands	EUR 387,234.48 / EUR 387,234.48

Based on the above facts it can be stated that no such ML cases were produced which would include the involvement of tax havens, however, this fact must be assessed within the overall threat resulting from the assessment of individual types of criminality.

The comparison of legal assistance volume for all criminal offences shows that in particular **Poland, USA, Romania, Spain, Switzerland and Ireland** have to be added to the above-mentioned States as regards the need to obtain evidence abroad. On the contrary, in addition to the above States, in particular **Bulgaria, Belgium and Ukraine** request assistance from Slovakia.

In the area of international cooperation, Slovak authorities are ever more frequently confronted with **requests for the seizure of proceeds, however, not only with the objective of future confiscation**. There is plenty of positive and negative experience within international cooperation, from practical problems (translation, speed of response) to deficiencies of the international legal regulation or national legal regulations insufficiently responding to commitments under international treaties. The application of the Warsaw Convention representing an important international tool is insufficient. Therefore, the Slovak representatives initiated the preparation of practical aids in the Committee of States Parties to the Warsaw Convention to facilitate its implementation which to a certain extent may help eliminate practical problems in identifying, seizing and confiscating proceeds of crime.

However, the problem of efficient cross-border cooperation also concerns the Convention on Cybercrime and other international contracts.

3.7. Services (products) used and sectors and institutions interested

These characteristics of ML cases distinguish services (products) and sectors and institutions interested, through which things, income or property should be placed into the "legal environment" during legalisation or sharing. Compared to the previous assessment, no big changes were found in this area. These tools (entities) were identified in individual ML cases as follows:

1. bank – use of accounts for transfers of financial resources coming from criminal activity (in particular unauthorised transfers, fraudulent withdrawals and phishing); these resources were subsequently transferred to other accounts, withdrawn in cash and then consumed or sent further through bank transfers of cash or using the Western Union service,

2. possession and use – the things coming from criminal activity were knowingly directly used (vehicles, appliances, etc.) or consumed, in some ML cases (vehicles), the origin of the thing was concealed (VIN tampering, use of other licence number), or such things were dismantled and their parts were further used; there were also ML cases, when things from criminal activity were possessed by the perpetrator (in particular vehicles) for the purpose of common sale, use or consumption,
3. common sale – acquisition or subsequent sale of a thing coming from criminal activity in the form of "common sale" (street sale, through friends, by advertising, through other people, etc.), in particular by contacting particular persons,
4. originality check – legalisation of a stolen car through originality check points[55], where during originality check a stolen vehicle was detected, or stolen vehicles were legalised at some points of originality check and then sold,
5. District Traffic Inspectorate and District Office – it was similar to "originality check", when during the registration of a vehicle in the records of vehicles at a PF department (after the sale or declared import from abroad) it was found out that the vehicles had been stolen, and there were cases, when a stolen car was detected at the respective department of road traffic of at a District Office,
6. courier - ML cases of possession, in which perpetrators were expressly selected for the transportation of stolen things (in particular vehicles) instead of their further sale or consumption, and perpetrators were detected mainly when crossing the State border of the SR,
7. gambling venue – by using slot machines, financial resources were legalised (stained banknotes from another criminal activity used for a game); it was one specific case, where the operator of the company operating slot machines pulled stained banknotes out of a machine in the amount of EUR 50.00,
8. pawnshop – things coming from criminal activity were placed in a pawnshop by the perpetrator, in an effort to obtain cash.

Out of all ML cases, most frequently a bank transfer of cash was concerned (63.69 % of ML cases), possession and use (12.80 % of ML cases), ML cases in connection with legalisation of stolen vehicles (originality check, District Traffic Inspectorate and District Office, together with a share of 12.20 %) and common sale (6.85 % ML cases). Other sectors occurred only sporadically.

[55]Originality checks are performed pursuant to Act No. 725/2004 Coll. on conditions of road traffic operation of vehicles and on the amendment to certain acts as amended

3.8. Identification of threats in individual sectors

3.8.1. Banking sector

Banks operating in the territory of the SR normally offer a wide portfolio of products for their customers. Modern technologies enabling remote communication with banks – "internet banking", banking applications in mobile phones and devices "smart banking", as well as a wide offer of payment cards are currently most widespread.

Within the banking sector, we can speak about the following threats:

1. the level of threat is very significant- in particular the use of cash transactions with the possibility of cash deposits, when illicit income from various criminal activities (mostly of economic nature and tax crime) is deposited into accounts based on the statement that the financial resources come from economic activities,
2. the level of threat is medium significant- use of virtual currencies and virtual assets (abuse in connection with frauds, organised crime, cybercrime) and cashless transactions (cross-border transfers connected with tax havens),
3. the level of threat is significant – private banking (above-standards banking and financial services, "anonymity" of the customer), safe deposit boxes (hiding proceeds obtained from illicit criminal activities), sector of electronic money (use of prepaid cards to which customer due diligence does not apply), transfers of money (remitting money through the providers of Money Value Transfer Services, use of front men) and payment services (frauds connected with payment cards, POS - terminals).

3.8.2. Sector of non-financial businesses and professions

Obliged entities for the non-financial sector are provided in Article 5 of the AML Act and include, for example, barrister, notary public, court executor, auditor, tax advisor, accountant, gambling operator, etc.

In terms of ML, a certain threat is represented in particular by companies with free trade licences, such as an organisational and economic advisor, accountant, legal person or natural person authorised to trade in precious metals or precious stones (purchase and sale).

Executive officers of companies with the above objects as well as lawyer's offices establish companies in Slovakia (mostly limited liability companies) with a wide and identical scope of various objects of company, for which they open bank accounts with the service of electronic banking offered automatically. Subsequently, according to demand and supply, they transfer them to persons from abroad, where business interests are transferred to a new owner without consideration. The established companies are mostly without employees, their registered office is at a "lucrative address" (the site is proportional to price) and high turnovers are recorded on accounts. After they receive a notice of control to be performed by the FIU SR or tax authorities, the movements on accounts are stopped, and the remaining financial resources are withdrawn in cash through an ATM. Establishment of such companies with

almost identical objects of free trade licences, with a registered office at a common address, represented by a foreign Executive Officer and partner, is on the rise, which represents the biggest threat in the non-financial sector.

3.8.3. Sector of other financial institutions (OFI)

The biggest ML threat in the OFI sector is the provision of products or services based on payment in cash or providing the possibility of payment in cash. This possibility occurs (except for an exchange) in all categories of the sector. Limitation of cash payments[56] in the OFI sector does not apply to cash payments made in exchange offices, payment institutions, payment service agents and electronic money institutions, and during auctions.

The other categories of the OFI sector can receive cash payments unless they exceed an amount of EUR 5,000.00. According to the performed survey, obliged entities endeavour to eliminate this way of payment to a minimum scope or they do not permit it at all based on internal regulations. On the other hand, however, the legislation allows the customer to make a deposit in cash into an account of a legal person kept by a financial institution, where the employee of the financial institution will not sufficiently verify the origin of deposited resources.

An ML threat can also be seen in security deposit paid for an auction in cash; the auctioneers do not examine the origin of paid financial resources. Payment institutions and payment service agents, i.e., the entities providing payment services based on cash payments or international cashless transfers (Western Union) represent another threat.

In general, the following types of criminal activity were identified in OFI sector categories:

- financial agent/advisor – frauds, credit frauds, insurance frauds, forgery and fraudulent alteration of an official document,
- factoring- tax criminal offences, frauds,
- leasing – tax criminal offences, frauds,
- creditor – frauds, forgery and fraudulent alteration of an official document,
- payment institutions, payment service agent and electronic money institutions - frauds, phishing.

It is only an assessment of a threat potential of the OFI category without underlying statistical data, which is not available to the country.

3.8.4. Insurance sector

In terms of ML threat, the insurance sector can be assessed as less attractive compared to the banking sector. The financial resources related to insurance policies (premium, payment of indemnity) are transferred from or to customers' accounts kept in other financial institutions which are obliged entities according to the AML Act. Premium is paid in cash (and only to a

[56] Act No. 394/2012 Coll. on limitation of cash payments

limited extent) only for some insurance products (e.g., travel insurance, collision insurance, and mandatory contractual insurance); the scope of premium received in cash in the SR is negligible compared to the total volume of premium received.

In assessing the level of ML threat in the insurance sector, a distinction should be made between the products in non-life insurance and life insurance products. It results from the application practice that the use of **non-life insurance** products for ML is very low; therefore, the level of ML threat can be designated as insignificant.

Compared to non-life insurance, the level of ML threat in life insurance represents a higher risk, in particular in unit-linked life insurance. The increased ML risk results in particular from the possibilities of investments by customers in the form of one-time deposits or repeated deposits and withdrawals. These products are primarily linked to the investment component of the contract and not to traditional insurance risk (death, survival). In consequence, the level of ML threat for **life insurance** products can be assessed as moderately significant. It means that the risk of legalisation in this area is present, however, to a limited extent, taking into account the size of the insurance sector within the financial market, character of insurance products, potential customers, selling channels, as well as the sufficient regulation of the insurance sector.

3.8.5. Sector of securities

The capital market represents a part of the financial market, where the movement of securities takes place; the medium-term and long-term capital, i.e., a low-liquidity capital is the subject of trading. Currently, trading in bonds prevails in Slovakia's financial market, trading in shares is represented to a smaller extent.

Securities traders and management companies administer various types of financial instruments; however, transfers are carried out by cashless operations, i.e., any financial transactions are carried out via the customers' bank accounts. For that reason, the customers, besides the monitoring by securities traders (or management companies) are also subject to monitoring by the banks or financial institutions, which make payments to customers' orders in favour of the respective customers' accounts.

To carry out business transactions, knowledge and expertise is necessary; therefore, perpetrators do not prefer this way of money laundering and terrorist financing.

Taking into account the above, the level of ML threat in the securities sector represents a **less significant risk**.

3.9. Number of cases cleared up

Out of the total number of 336 prosecuted ML cases, in total 64 ML cases were cleared up (19.05 %), i.e., a bill of indictment was filed or the investigation was terminated in a way reported as cleared up, although no particular person was charged (e.g., due to the inadmissibility of criminal prosecution, absence of a witness, transfer of criminal prosecution abroad).

3.10. Number of entities involved

In the assessed period from 2016 to 2019, 491 Slovaks and 368 foreigners participated in prosecuted ML cases. It is the number of persons participating in the cases, i.e., persons without an exact specification of procedural position, thus the persons participating in an ML case directly or indirectly were not necessarily charged or suspicious.

3.11. Conclusions of the analysis of the assessed criminal prosecutions of legalisation of proceeds of crime

The analysis of assessed cases showed that frauds committed in particular abroad with the subsequent unauthorised transfer of financial resources represented the biggest part of predicate criminal offences. Theft of a thing, most frequently in connection with thefts of motor vehicles, was another most frequent form of commission of predicate criminal offences.

ML cases and predicate criminal offences were not committed by State authorities, legal or similar sectors, stock exchange, etc.

Commission of ML cases and their predicate criminal offences was mostly performed in the territory of the SR, and from the view of possible clear-up rate, the international element only occurred to a limited extent.

The finding that only exceptionally ML cases or their predicate criminal offences were recorded, which were committed in connection with criminal offences of economic character, tax crime, and well-organised perpetrators of criminal offences (organised crime), is worth mentioning. No cases in which predicate criminal offences would be committed by violence or threat of imminent violence or by extortion were carried out in the monitored period.

ML cases:

- the number of ML cases did not change very much during the monitored period,
- two cases of a failure to notify or report were detected in the monitored period,
- the most widespread method used for legalisation in the investigated ML cases was the unauthorised transfer of financial resources through bank institutions or by using their services, the second most widespread method of commission was carried out in connection with (stolen) motor vehicles,
- the convicted ML cases concerned in particular VIN tampering in motor vehicles stolen in the SR or abroad, their registration based on false certificates of registration or dismantling them to spare parts for the purpose of possession, use or sale, in the banking sector, in particular transfers of money obtained in a fraudulent way (often abroad) to bank or game accounts, submission of false invoices and subsequent withdrawal of financial resources for the purpose of possession, sale or direct consumption; even more sophisticated techniques using “straw men” for bank account opening, using internet systems (e.g., illicit obtaining of personal data abused for frauds), as well as using business companies were recorded.

Predicate criminal offences:

- predicate criminal offences were most frequently committed in the form of various fraudulent activities (frauds), in particular abroad, with the subsequent unauthorised transfer of financial resources, these are followed by thefts, where perpetrators were interested mainly in motor vehicles,
- on the contrary, the convicted ML cases included thefts, falsification and fraudulent alteration of motor vehicle identification numbers in the automotive sector, as well as frauds and counterfeiting and altering a public instrument in particular in the banking and tax sectors,
- as regards predicate criminal offences, there was only one case committed in a sophisticated way, no commission of criminal violence was confirmed.

In terms of a lower number of serious cases of criminal prosecution of legalisation of proceeds of crime, it can be stated that:

- It is a state determined by several factors; only a small part of them can be affected by the investigators of the PF SR, FACO and bodies of the Prosecutor's Office. **Despite the measures taken in response to the Action Plan to Combat Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction for 2019 to 2022, there was no success in sufficiently focusing on and creating related organisational and material preconditions for systematic search for and detection of potential laundering from early stages of unlawful activities based on an efficient proactive financial investigation taking into account the ML threat and risks identified.**
- In the cases of serious organised criminal activity, pre-trial proceedings last longer, often several years, therefore, the submitted statistics does not take into account many cases with a pending criminal prosecution for the criminal offence of legalisation of proceeds of crime because the pre-trial proceedings have not been concluded yet (filing a bill of indictment) and the perpetrator has not been convicted. **The length of proceedings is among the threat factors determining the efficiency in this area.**
- The length of proceedings is also determined by legislative-system issues of the scope of criminalisation of criminal social conduct and related scope of occurrence of individual cases in relation to available forces and means. Thus, often a situation occurs in practice that investigators and prosecutors focus on cases in which the taking of evidence is simpler, in particular in investigating predicate criminal offences; **in the absence of efficient financial investigation, they are satisfied with the conclusion of a case to an extent of predicate criminal offence**.
- Knowledge from practice repeatedly shows that the seizure of proceeds of crime in our conditions is really executable only if the course of commission of the criminal activity is subject to procedural acts of criminal proceedings, otherwise **the proceeds of the criminal offence quickly disappear and vanish away on various accounts kept for persons not interested and uninformed**, or their further movement is covered by

operations seemingly legal, when it is also impossible to contest the legal reason for payment.

- "Straw men", with a low intellectual capacity, for whom intentional culpability cannot be proved even if in the form of indirect intent, are often involved in disposing of the proceeds of crime.
- In most cases, it is very difficult to **identify the perpetrators of predicate criminal offences**, nor it is possible **to identify finally the form of money laundering**, i.e., to determine whether the person, who fraudulently elicited money, is **the same (or other) person as the person, who subsequently handled the resources** as the owner/person authorised to dispose of the bank account concerned. The way of commission of some of these acts suggests that **several persons acting in a coordinated way in various States are concerned**, or that this **activity is committed through organised groups.**
- The (often **purposive) insolvency of perpetrators**, who do not have any property because the income from criminal activities was spent on gambling, payment of old debts, etc., is another frequent reason for a failure to seize proceeds of crime or property obtained within criminal activities.
- The placing of proceeds and their transfer to third persons from the beginning of unlawful conducts (legalisation aspect) fully escapes.
- Spreading of criminal offences against morality which is an important factor of ML threat.
- THE QUALITY OF REALLY INVESTIGATED AND PROSECUTED CASES OF LEGALISATION OF PROCEEDS OF CRIME DID NOT REFLECT THE GRAVITY OF THE DETECTED PREDICATE CRIMINAL ACTIVITY.
- COMPARED TO THE 1ST ROUND OF NRA, WHEN THE WITHDRAWAL OF PROCEEDS BY DIRECT INSTRUMENTS IN ML CASES WAS IMPOSED ONLY TO A MINIMUM EXTENT, THERE WAS A POSITIVE CHANGE IN THE NUMBER AND VOLUME OF SEIZURE OF PROCEEDS OF CRIME.
- Despite a positive trend in imposing property-related penalties, the progress is not sufficient and real withdrawal of proceeds of crime still marginally affects the proceeds generated by criminal activities or in a broader context, circulation of "dirty money" in the economy.
- The analysis unambiguously confirmed the fact that despite the capability to penalise all types of legalisation (self-laundering, autonomous money laundering or money laundering by third persons), including the penalisation of legalisation of proceeds generated by criminal activities abroad, and even despite an increase in the number of investigations, criminal prosecutions and convictions for legalisation of proceeds of crime, **the majority of cases concerned simple property-related criminal offences**, and the share of **High Profile Cases** increases only gradually.
- In general, despite the adoption of several measures, no stable positive trend in the area of quantitative increase in the number of cases detected, investigated or with conviction in this area can be stated in the period 2016-2019.
- Penalising the legal persons for the legalisation of proceeds of crime still remains a challenge.

- However, we have registered a qualitative change at the end of 2019 and in 2020; in addition to other factors, it should be imputed to the functioning of measures adopted within the fulfilment of the action plan for the previous NRA (e.g., in the area of financial investigation, in the area of mentality change, adjustment of law enforcement authorities focusing on the application of the follow-the-money principle). In this period, several criminal prosecutions were commenced for the organised form of corruption and other types of criminal offences of economic nature (but for example, also environmental crime) perpetrated in an organised form including the related moment of legalisation of proceeds of crime generated in such a way. However, in the process of NRA performance, these criminal cases were mostly in pre-trial proceedings or final court decisions were not available yet.
- Legal persons are often used as means of legalisation but **no legal person has been finally convicted of** ML yet; however, some investigations are pending.
- Despite several convictions concerning organised crime, trafficking in human beings and drugs, the results of penalising the proceeds generated in an organised form of crime are modest.
- Absolutely in conflict with the threat identified by the previous NRA – no substantial results were achieved in prosecuting and convicting ML cases in connection with corruption. In this area, too, a positive trend has been recorded since the end of 2019.
- The absence of real proactive parallel financial investigation from the earliest stages of illicit conduct and consumption of an act of simple legalisation form to a predicate criminal offence is the biggest source of inefficient system of detection and generation of serious cases of legalisation of proceeds of crime.

-

4. The most important threats and related trends

In assessing and determining money laundering threats, the group used as a basis **the overall contexts of long-term development of criminality** in the conditions of the SR, which were affected by many factors having impact on the commission of criminal activity. However, primarily it is the motive of perpetrators to generate profits (proceeds), i.e., the reason why they commit the criminal offence, and **the determination of the potential of a type of crime as a source area of the generation of proceeds of crime**.

Based on the above mentioned, the **assumed amount of unrecorded proceeds** was determined, and **FRAMEWORK ML THREATS** AND RELATED **TRENDS** were set:

Criminality / criminal offence	Assumed amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium-low	Low	no change	Upward	Downward
Criminal violence	except for carrying concealed weapons and arms trafficking, where the proportion of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for criminal violence is not significant				X				X
Premeditated murder Article 144	insignificant					X			X
Murder Article 145	insignificant					X		X	
Robbery Article 188	insignificant				X				X
Extortion Article 189	insignificant				X				X
Gross coercion Articles 190, 191	insignificant					X			X
Prohibited acquisition and possession of firearms and trafficking in them Article 294	substantially higher		X				**X**		
Prohibited acquisition and possession of firearms and	substantially higher		X				**X**		

trafficking in them Article 295									
Criminal offences against morality	except for THB, where the proportion of unrecorded proceeds is higher, the proportion of unrecorded proceeds is not significant for criminal offences against morality				X			X	
Pimping Article 367	slightly higher			X			X		
Production of child pornography Article 368	estimate impossible				X			X	
Dissemination of child pornography Article 369	higher				X			X	
Possession of child pornography Article 370	insignificant					X	X		
THB Article179	higher				X		X		
Criminal offences against property	the proportion of unrecorded proceeds is slightly higher				X				X
Theft Article 212	slightly higher				X				X
Failure to pay wages and redundancy payment Article 214	insignificant					X			X
Unlawful enjoyment of a thing of another Article 215	insignificant					X			X
Criminal offences of economic nature	the proportion of unrecorded proceeds is (disproportionally) higher		X				X		
Embezzlement Article 213	insignificant			X					X
Unlawful manufacturing and enjoyment of payment means, electronic money or other payment card Article 219	insignificant			X			X		
Fraud Article 221	higher		X						X
Credit fraud Article 222	slightly higher					X			X
Insurance fraud Article 223	higher					X			X
Subsidy fraud Article 225	higher		X					X	

Unjust enrichment Article 226	insignificant					X			X
Fraudulent bankruptcy Article 227	substantially higher		X						X
Induced bankruptcy Article 228	higher				X		X		
Usury Article 235	slightly higher			X			X		
Forgery, fraudulent alteration and illicit manufacturing of money and securities Article 270	slightly higher				X		X		
Tax and insurance premium evasion Article 276	higher	X							X
Failure to pay tax and insurance premium Article 277	higher		X				X		
Tax fraud Article 277a	higher		X				X		
Failure to pay tax and insurance premium Article 278	higher			X				X	
Counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark Article 352	insignificant					X	X		
Abusing participation in economic competition Article 250	higher					X	X		
Unlawful business activity Article 251	slightly higher				X		X		
Unlawful employment Article 251a	insignificant					X	X		
Unlawful trading in foreign currency and providing foreign-exchange services Article 252	insignificant					X	X		
Breach of regulations governing imports and exports of goods Article 254	insignificant			X			X		

Breach of regulations governing the handling of controlled goods and technologies Articles 255, 256, 257	insignificant					X	X		
Distortion of data in financial and commercial records Article 259	higher			X			X		
Damaging the European Communities' financial interests Article 261	slightly higher			X				X	
Endangering trade, bank, postal, telecommunication and tax secrets Article 264	insignificant					X	X		
Insider trading Article 265	slightly higher				X		X		
Contrivance in public procurement and public auction Articles 266, 267, 268	slightly higher			X				X	
Harm caused to a consumer Article 269	insignificant					X			X
Environmental crime	the proportion of unrecorded proceeds is (disproportionally) higher		X					X	
Illicit manufacturing and possession of nuclear materials, radioactive substances, hazardous chemicals and hazardous biological agents and toxins Articles 298, 299	estimate impossible			X			X		
Unauthorised construction Article 299a	higher			X			X		
Endangering and damaging the environment Articles 300, 301	substantially higher		X					X	

Unauthorised handling of waste Article 302	substantially higher	X						X	
Unauthorised discharge of pollutants Article 302a	substantially higher		X				X		
Breach of water and air protection Articles 303, 304	substantially higher		X				X		
Unauthorised production and handling of ozone-depleting substances Article 304a	higher			X			X		
Breach of plant and animal species protection regulations Article 305	higher				X		X		
Breach of trees and shrubbery protection regulations Article 306	higher		X					X	
Spreading on a contagious disease of animals and plants Articles 307, 308	insignificant					X	X		
Escape of genetically modified organisms Article 309	insignificant					X	X		
Poaching Article 310	higher			X			X		
Endangering health due to decayed foodstuffs and other items Articles 168, 169	insignificant					X	X		
Theft (only in relation to timber pursuant to Article 212 (1) (e)	substantially higher		X					X	
Inflicting cruelty to animals Article 378	insignificant					X	X		
Breaching the duty of care of animals Article 378a	insignificant					X	X		
Corruption crimes	the proportion of unrecorded proceeds is higher		X				X		

Abuse of power by a public official Article 326	higher			X					X
Receiving a bribe Article 328	higher			X					X
Receiving a bribe Article 329	higher			X			X		
Receiving a bribe Article 330	higher			X					X
Bribery Article 332	higher			X			X		
Bribery Article 333	higher			X					X
Bribery Article 334	higher			X					X
Trading in influence Article 336	higher			X					X
Electoral corruption Article 336a	slightly higher				X				X
Corruption in sport Article 336b	insignificant				X				X
Organised crime	the proportion of unrecorded proceeds is substantially higher	X							X
Establishing, masterminding and supporting a criminal group Article 296	substantially higher		X				X		
Human smuggling Articles 355, 356	substantially higher	X							X
Drug-related crime	the proportion of unrecorded proceeds is substantially higher		X					X	
Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors Article 171	insignificant				X		X		
Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors Article 172	substantially higher		X					X	

Illicit production, holding of and trafficking in narcotic drugs and psychotropic substances, poisons or precursors Article 173	substantially higher			X			X		

5. Money laundering vulnerability of the country

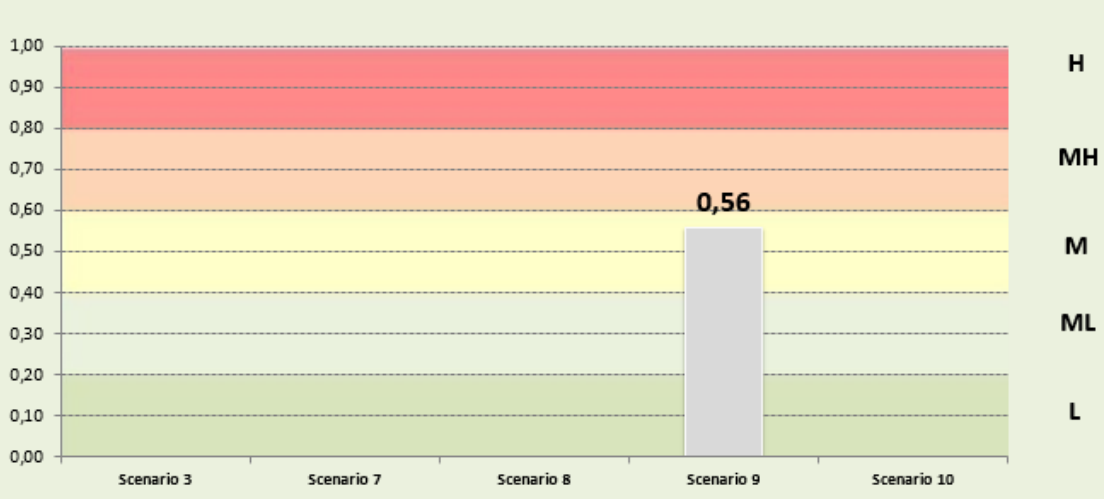
The country's vulnerability assesses the mechanisms of measures used by the SR in combating money laundering. To assess vulnerability, the World Bank's programme tool was used as a support. The assessment of the country's vulnerability should help:

- create an action plan to improve the efficiency of the fight against ML,
- evaluate the influence of various interventions of regulatory and other relevant authorities,
- compare the level of vulnerability of evaluated sectors,
- ensure efficient allocation of resources.

Overall ML vulnerability at national level

The overall vulnerability of the SR was assessed based on the ability of the country to fight against legalisation and on the overall vulnerability of national economy sectors. The overall money laundering vulnerability of the country was assessed as medium-level (a score according to the programme tool: 0.56), which represents only a moderate improvement compared to the previous NRA for the assessment period 2011 to 2015 (a score according to the programme tool: 0.6).

ML vulnerability at national level



ML vulnerability at national level, within a scale of 0 – 1, a higher value means higher vulnerability

5.1. The country's ability to combat legalisation of proceeds of crime

The country's ability to combat legalisation of proceeds of crime (hereinafter the "legalisation") represents the country's ability to criminally prosecute and penalise the cases of criminal offence of legalisation and the country's ability to seize proceeds and means of criminal activity. The country's ability to combat legalisation was evaluated at medium level (a score according to the programme tool: 0.48)**.** (Within the NRA for the assessment period from

2011 to 2015, the country's ability to combat legalisation was at a medium-low to medium level, a score according to the programme tool: 0.4).

The SR's ability to combat legalisation was evaluated on the basis of the assessment:

- of input variables directly affecting the quality of general measures against legalisation at national level
- of mixed variables evaluated by the MODULE 2 programme tool. The input and mixed variables are displayed in the map of vulnerability.

Input variables affecting the country's ability to combat ML	Score
Quality of AML policies and strategies	0.6
Efficiency of the definition of the criminal offence of legalisation of proceeds of crime	0.7
Comprehensiveness of legal framework for seizure of property	0.5
Quality of the FIU SR activity in obtaining and processing intelligence information	0.6
Capacities and resources for the investigation of financial criminal activity	0.4
Integrity and independence of investigators	0.6
Capacities and resources for criminal prosecution of financial criminal activity	0.5
Integrity and independence of prosecutors	0.6
Capacities and resources for court proceedings concerning financial criminal activity	0.5
Integrity and independence of judges	0.4
Quality of border checks	0.7
Comprehensiveness of the customs procedure in controls of cash and similar instruments	0.7
Efficiency of customs controls during transport of cash and similar instruments	0.7
Efficiency of national cooperation	0.5
Efficiency of international cooperation	0.8
Level of national economy formalisation	0.7
Level of financial integrity	0.7
Efficiency of tax collection	0.5
Availability of independent audit	0.7
Availability of credible identification infrastructure	0.6
Availability of independent information resources	0.6
Availability of information on beneficial ownership	0.6

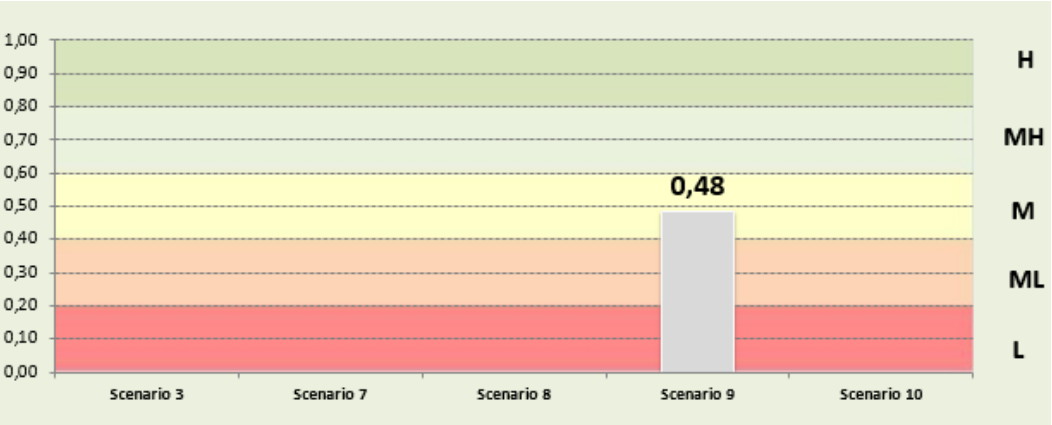
Mixed variables affecting the country's ability to combat legalisation:

A. Quality of AML policies and strategies
B. Efficiency of the definition of the criminal offence of legalisation
C. Efficiency of cross-border controls of cash
D. Quality of detection of criminal offences
E. Quality of criminal prosecution
F. Quality of judgements
G. Quality of framework for property seizure and withdrawal of proceeds of crime.

The results of the evaluation of the above factors identified in particular an insufficient quality of judgements, insufficient capacity and insufficient resources for the investigation of financial criminal activities, a lower quality of investigation of criminal activities, criminal prosecution, seizure of property and withdrawal of proceeds of crime.

The ability to combat ML at national level, within a scale of 0 – 1, a higher value means higher ability to combat ML

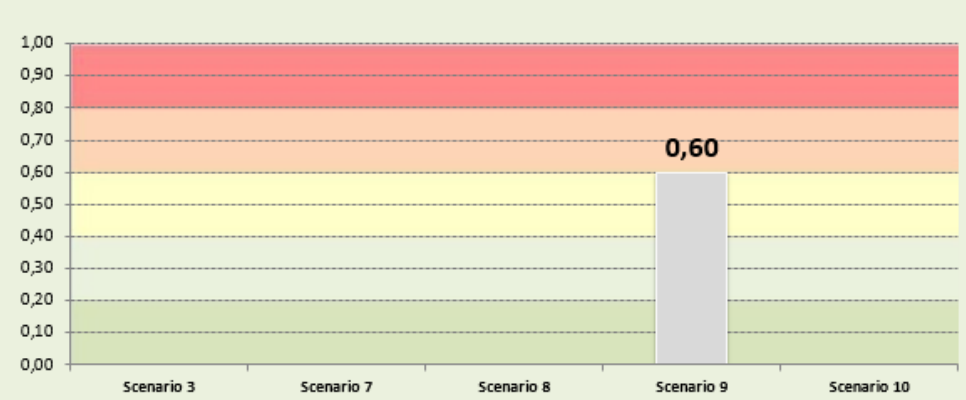
Ability to combat ML at national level



5.2. Overall vulnerability of sectors

The overall vulnerability of sectors was evaluated at a medium to medium-high level, a score according to the programme tool: 0.60. (For the NRA in the assessment period 2011 to 2015, the overall vulnerability of sectors of the country was at a medium to medium-high level, a score according to the programme tool: 0.61). Vulnerability was assessed by working groups for the following sectors: banks, insurance companies, securities traders, management companies, payment institutions (along with electronic money institutions and payment institution agents), exchange offices, gambling operators, real estate agencies, traders in precious stones, auditors, accountants, notaries public, barristers, leasing companies, financial agents and financial advisors, tax advisors, creditors, legal persons or natural persons authorised to organise auctions except for executions, and legal persons and natural persons authorised to provide organisational and economic consulting. The highest vulnerability was assessed in the banking sector (a medium-high level of vulnerability, score: 0.62), the sector of management companies and sector of legal persons and natural persons authorised to provide organisational and economic consulting followed (a medium level of vulnerability, score: 0.58), the sector of financial agents and financial advisors (a medium level of vulnerability, score 0.55), and the sector of traders in precious metals (a medium level of vulnerability, score 0.55).

Overall sector ML vulnerability



Overall sector ML vulnerability, within a scale of 0 – 1, a higher value means a lower ability to combat ML

The following vulnerabilities were identified in the banking sector:

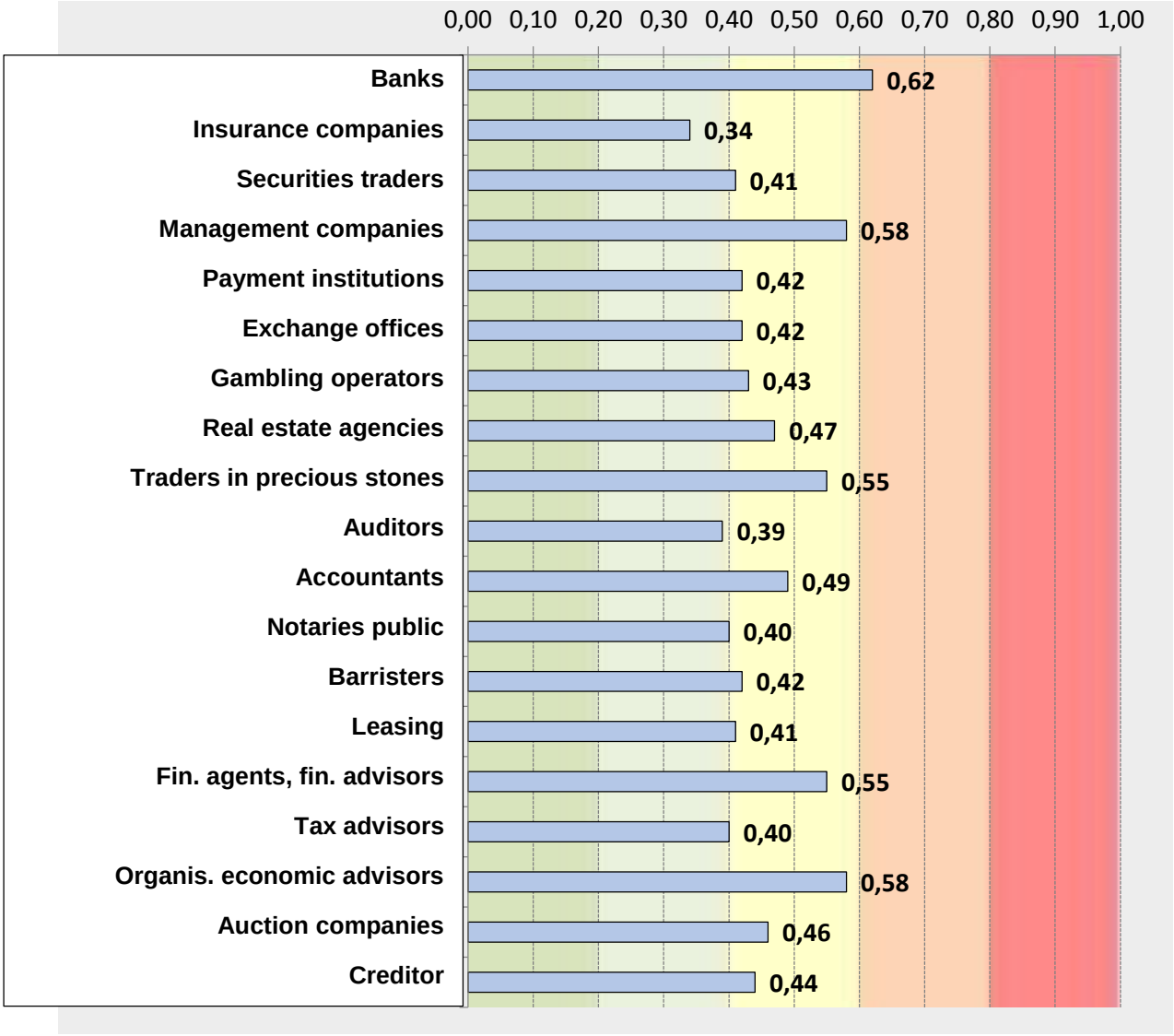
- in providing private banking services, banks sent unusual transaction reports (hereinafter "UTRs") concerning private banking customers to a very limited extent,
- insufficient enforceability of Act No. 394/2012 Coll. on limitation of cash payments,
- a low number of reported UTs concerning politically exposed persons; banks should focus on the process of provision of customer due diligence in more detail, in particular if the customer does not use other products of the bank, they should obtain as much information as possible on the purpose and nature of the business relationship with the customer (expected frequency of visits, the relationship between the owner and the person authorised to dispose of the safe deposit box, finding the reason for using the safe deposit box, etc.,
- banks should precisely monitor the transactions with crowdfunding signs,
- high dynamics of development and technological changes in virtual assets, non-existent/insufficient regulation in this area, anonymity of the environment,
- a high level of vulnerability, which means a high risk of abuse of a particular product for the purposes of legalisation, was found for payment accounts of legal persons (small and medium enterprises).

Factors considerably affecting the vulnerability in several assessed sectors include:

- insufficient obliged entities' awareness of ML/FT risks and their management,
- preferring the business policy to the AML policy,
- a failure to observe legislation,
- insufficient determination of the origin of financial resources or property during customer due diligence,
- insufficient number of performed controls of obliged entities and pooled asset funds.

The result of an overall country's ML vulnerability at national level points out the fact that the level of measures in combating money laundering is at an average level and like in the

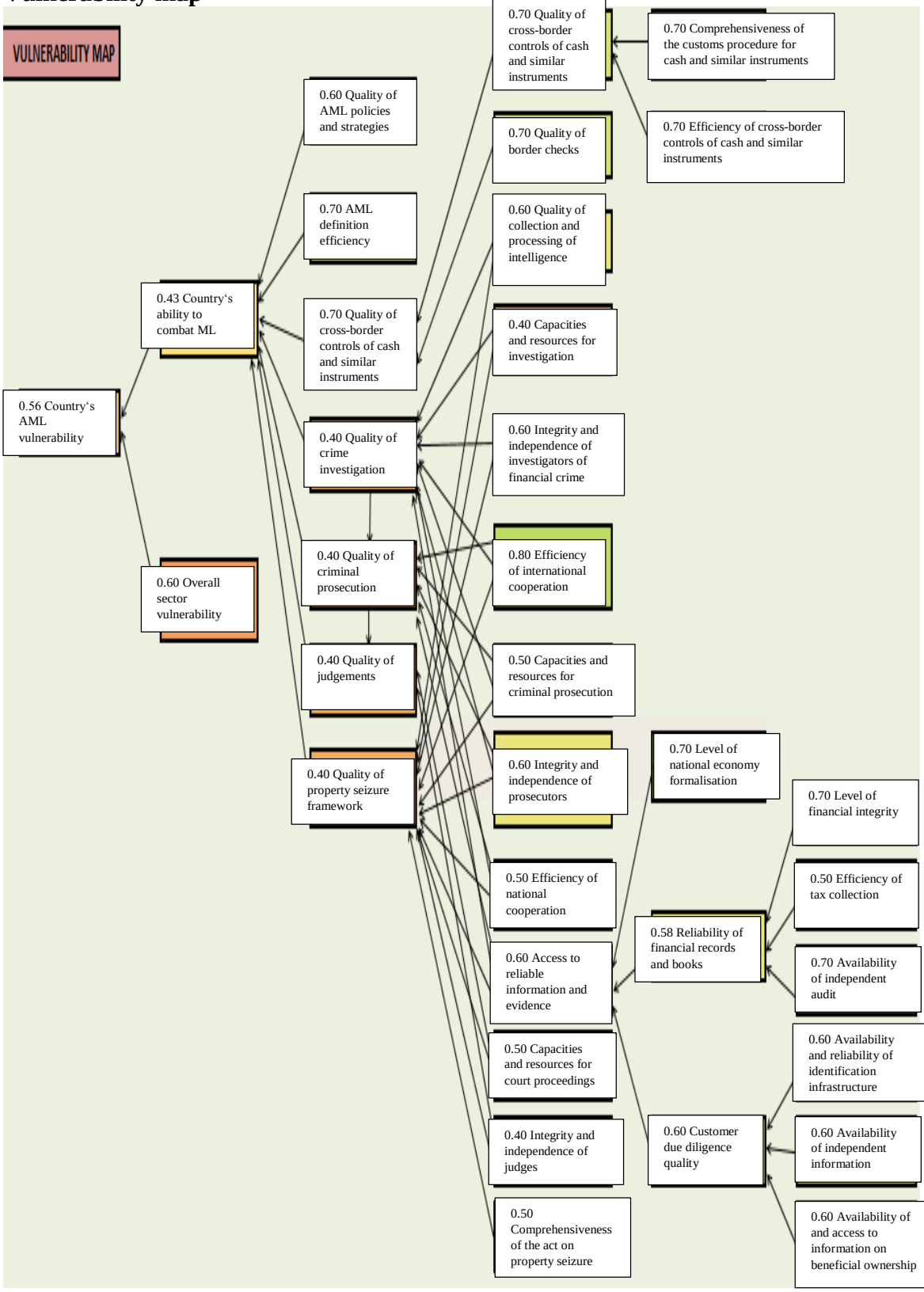
previous NRA (for the assessment period 2011 – 2015), a lower efficiency of the measures was found.



Vulnerability of evaluated sectors

The vulnerability map is a visual summary of assessment; it shows the values of individual factors affecting the country's overall vulnerability. The assessment results displayed in the vulnerability map show that the overall AML vulnerability of the SR is at a medium level, and the overall sector vulnerability is at a medium to medium-high level. The country's ability to combat legalisation was evaluated as a medium level.

Vulnerability map



5.3. Factors affecting the country's ability to combat legalisation

A. Quality of AML policy and strategy

In its Manifesto of the Government for the period 2016 - 2019, the Government of the SR undertook to adopt further measures to combat legalisation. The National AML/CFT Expert Group (hereinafter "NES-LP") established by the Interdepartmental Expert Coordination Body for Combating Crime (hereinafter "MEKO") fulfilled important tasks in improving the efficiency and effectiveness of these measures in the assessment period from 2016 to 2019. MEKO is a national authority ensuring the fulfilment of tasks in combating criminality resulting from programme documents of fight against criminality, from the Manifesto of the Government of the Slovak Republic, from international legal acts and treaties binding on the Slovak Republic. MEKO also initiates the preparation of legislative proposals for the improvement of interministerial cooperation in combating criminal activities. The AML/CFT policies and activities are among the many areas coordinated by MEKO. NES-LP is led by the FIU SR Director, and it includes NBS, MF SR, MJ SR, GPO SR, Ministry of Economy of the SR, MD SR and other institutions. Most institutions contributing to the activity of NES-LP are considered AML/CFT policy-makers.

In 2017, a subgroup for fight against terrorist financing and proliferation of weapons of mass destruction was established within NES-LP. This subgroup is responsible for analysing the state in the area of terrorist financing and proliferation of weapons of mass destruction, for preparing the rules of information exchange among the members in this matter, and for identifying defects in the mechanisms of fights against terrorist financing and proliferation of weapons of mass destruction.

In February 2018, a murder of a journalist and his fiancée was committed in the SR. The murder affected the whole society, rearrangement of political power, the police started investigating prominent perpetrators, negotiations started about the reform of the judicial system, and law enforcement authorities started investigating serious criminal offences of economic nature including the criminal offences of legalisation of proceeds of crime to a greater extent.

For the first time, the SR identified and assessed ML/TF risks at national level based on the National Money Laundering and Terrorist Financing Risk Assessment for the assessment period 2011 to 2015 (hereinafter "NRA 1"). Based on the results of NRA 1, the Action Plan to Combat Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction for 2019 to 2022 (hereinafter the "Action Plan") was prepared, which was approved by Government Resolution of the Slovak Republic No. 207/2019 dated 7 May 2019, in which the Government of the SR also took note of the NRA 1 Report. Strategical Principles of Fights against Money Laundering and Terrorist Financing in the SR for the period 2019 to 2024 were attached to the Action Plan; the 17 strategic principles represent an expert proclamation of the direction of activities of competent authorities fulfilling their AML/FT tasks and duties.

The second National Money Laundering and Terrorist Financing Risk Assessment in the SR (hereinafter "NRA 2") was commenced on 15 May 2020 in compliance with Article 26a of Act No. 297/2007 Coll. on the protection against the legalisation of proceeds of crime and terrorist financing and on the amendment to certain acts as amended. NRA 2 had to be carried out also on the basis of Task C. 36 from the Action Plan and the MONEYVAL Committee, a permanent monitoring body of the Council of Europe to counter money laundering and the financing of terrorism, also called upon the SR to perform it.

For NRA 2 performance, the MEKO Secretariat expanded the NES LP working group involving a wide spectrum of various institutions. Eight working teams were created for the NRA 2 Project. Three working teams fulfilled the tasks of global character (identification of threats and vulnerabilities in the system of measures against legalisation and assessment of measures in the fight against terrorism) and five working teams assessed individual sectors (banking sector, sector of securities, insurance sector, sector of other financial institutions, sector of non-financial business and professions). Representatives of the Financial Intelligence Unit acted as leaders of working groups within NRA 2.

The NRA 2 process was affected by the epidemiological situation in the SR, when the second wave of the COVID-19 pandemic limited meetings of working groups to a distance form.

The summary of most important legislative measures:

In an effort to efficiently respond to the constant development in ML/TF, the adoption of an amendment to the AML Act based on Act No. 52/2018 Coll. transposing Directive (EU) 2015/849 of the European Parliament and of the Council was an important measure, at the same time, some recommendations of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL and FATF recommendations were accepted. This amendment imposed the duty to register data on beneficial owners of legal persons upon several source registers, including the Commercial Register.

The adoption of Act No. 315/2016 Coll. on the register of public sector partners and on the amendment to certain acts, which came into effect on 1 February 2017, represented another AML measure. An important task of this act was to improve the transparency in transactions of entities participating in public procurement or doing business with the State. Based on the above act, the duty to publish beneficial owners was imposed upon the entities doing business with the State.

At the same time, based on an amendment to Act No. 757/2004 Coll. on courts (Article 82i), in 2016, a central register of disqualifications was created at the District Court Žilina. The register of disqualifications is a publicly available register, which is part of the central information system of the judicial system. Data on natural persons, who based on a decision on exclusion must not hold a position of a statutory body member, supervisory body member, manager of an organisational unit of the company, manager of an enterprise of a foreign person, manager of an organisational unit of an enterprise of a foreign person or a holder of procuration (so-called excluded representative) is registered in the register of disqualifications for a period

of disqualification (at least three years). The data on excluded representatives is obtained from the disqualification letters of courts of the Slovak Republic. The decision on exclusion is governed by Article 13a of the Commercial Code. The decision on exclusion is a decision determined by law – e.g., a final judgement imposing a penalty of ban on holding such position or a final judgement of the court in accordance with the Act on Bankruptcy and Restructuring deciding on imposing the duty on a statutory representative to pay a contractual penalty for the violation of the duty to file a petition for bankruptcy. These facts are examined by the competent register court in registering a statutory or supervisory body member, manager of an organisational unit of an enterprise/ of an enterprise of a foreign person or holder of procuration in the Commercial Register.

In addition to the legislative measures in relation to the Criminal Code and Code of Criminal Procedure (see more details in Part B and Part G), Act No. 91/2016 Coll., which came into effect on 1 July 2016, introduced criminal liability of legal persons into law of the SR. Based on this act, a legal person is also criminally liable for money laundering.

A draft act on the execution of asset seizure decision and seized asset management and on the amendment to certain acts has been repeatedly submitted to the legislative process since 2019. This act (Act No. 312/2020 Coll.) was eventually adopted in autumn 2020 and came into effect on 1 January 2021. Besides the establishment of the Office for Seized Asset Management expected on 1 August 2021, it also includes amendments to the Criminal Code, Code of Criminal Procedure, act on bankruptcy and settlement, act on criminal liability of legal persons and other acts with the objective to considerably strengthen the legislative framework for combating money laundering.

The measures carried out on the basis of the Action Plan are implemented continuously. Based on a task from the Action Plan, the Rules of Procedure and Statute of MEKO were updated for the purpose of more efficient operation of MEKO.

Vulnerability:

- insufficient allocation of resources necessary to implement measures to combat ML/TF.
- absence of prioritisation of more significant criminal prosecutions
- inconsistent withdrawal of proceeds of crime
- low efficiency of financial investigation

B. Efficiency of the definition of the criminal offence of legalisation of proceeds of crime[57]

Compared to the previous assessed period, no essential change of the concept of the criminal offence of legalisation of proceeds of crime occurred in the monitored period (Article 233, Article 234) except for a modification of Article 233 of the Criminal Code, where the words "criminal offence" are replaced by the words "criminal activity"; and the reference to "other property" in the text is replaced by the term "a thing coming from" (criminal activity). The objective of the changes was to allow penalising the legalisation of property coming from criminal activity, i.e., to not be bound to the condition of its origin strictly in the criminal offence according to law of the Slovak Republic in accordance with Article 8 of the Criminal Code.

It can be stated that the respective modification helped increase the efficiency of criminal prosecution of money laundering. However, the composition of cases within the Moneyval Evaluation showed that mostly cases of lower importance were concerned (see the Threats part).

In relation to predicate offences, the "*all crime approach*" was preserved, i.e., any criminal offence listed in the Criminal Code may be a predicate criminal offence.

The sentencing tariffs, types of penalties or principles of imposing penalties were not modified, either.

Criminal offence of legalisation of proceeds of crime in figures (Article 233 and 234 of the Criminal Code)

Year	Number of persons convicted	Average length of the sentence of imprisonment	
		The highest	The lowest
2016	18	96 months	24 months
2017	12	156 months	60 months
2018	6	56 months	0
2019	3	96 months	-

[57] The term "legalisation of proceeds of crime" replacing the term "legalisation of income from crime" is used in the whole text of the NRA Report. This change was carried out on the basis of Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts amending Act No. 300/2005 Coll. Criminal Code as amended, changing the name of criminal offence in Article 233 of the Criminal Code from the original term "legalisation of income from crime" to the term "legalisation of proceeds of crime" with effect from 1 January 2021.

However, the definition of the term "thing" (Article 130) was expended so that punishing essentially any property meeting the conditions for imposition of the penalty of forfeiture of a thing or protective measure of confiscation of a thing is enabled in practice.

The above changes were implemented by Act No. **397/2015** with effect from 1 January 2016.

The introduction of criminal liability of legal persons into law of the Slovak Republic by **Act No. 91/2016 Coll.** on criminal liability of legal persons with effect from 1 July 2016 was an especially significant change. This act is *lex specialis* in relation to the Criminal Code and Code of Criminal Procedure. Criminal liability is applied to legal persons only in relation to the criminal offences exhaustively listed in Article 3 of this act, which, in addition to the criminal offence of legalisation of proceeds of crime, also include key predicate criminal offences, such as criminal offences of corruption, terrorist financing, drug-related criminal offences or trafficking in human beings.

In the assessed period, criminal prosecution was commenced against legal persons (Article 199 of the Code of Criminal Procedure) and they were charged (Article 206 of the Code of Criminal Procedure) with the criminal offence of legalisation of proceeds of crime pursuant to Article 233 of the Criminal Code only in several cases: in 2016 – 0, in 2017 – 0, in 2018 - 2 cases (Article 233 of the Criminal Code) = commenced Article 199 of the Code of Criminal Procedure + Article 206 of the Code of Criminal Procedure, in 2019 - 1 case (Article 233) = commenced Article 199 of the Code of Criminal Procedure + Article 206 of the Code of Criminal Procedure. However, no legal person was convicted of the criminal offence of legalisation of proceeds of crime in the monitored period.

For an overall image, it should be noted that an essential reform of terrorist financing criminalisation was implemented by **Act No. 161/ 2018 Coll.** with effect from 1 June 2018. The culpability of terrorist financing is regulated in a separate criminal offence – terrorist financing in Article 419c of the Criminal Code.

Vulnerabilities:

It resulted from the Moneyval evaluation from 2019 that "there are discrepancies in the approach to the issue of the purposive element and coverage between the Conventions and the Criminal Code of the Slovak Republic" (read the Vienna and Palermo Conventions). Although it was recognised that this gap was to some extent mitigated by the offence of *"sharing"* in Article 231 of the Criminal Code, the scope of *"sharing"* was, however, considered as significantly narrower than the ML offence only applying to persons other than the perpetrator of the predicate offence. In consequence, the evaluators came to a conclusion that any ML acts committed by the offender with knowledge of the criminal source but without a demonstrable intent to conceal would be covered by neither Article 233 nor Article 231 and were therefore not criminalised. According to evaluators, this aspect also limits the scope of self-laundering.

The second aspect was the possibility of criminal sanction for an accomplice in committing the criminal offence of legalisation of proceeds of crime in the event that qualified

merits are not concerned, where Article 296 of the Criminal Code (criminal group) can be applied.

The above observations led to a national discussion about a conceptual change of the culpability of legalisation of proceeds of crime, which took place in parallel with the assessment process. The national discussion resulted in adopting Act No. 320/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts which also amended Act No. 300/2005 Coll., the Criminal Code, with effect from 1 January 2021**.** The analysis of this new regulation will be included in the next national risk assessment.

C. Efficiency of cross-border controls of cash

In the assessment period, the Slovak Republic used a system of reporting the incoming and outgoing transportation of cash and bearer negotiable instruments across external EU borders for natural persons. Regulation (EC) No. 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community applies directly to the SR; it is supplemented by provisions of Act No. 199/2004 Coll., Customs Act. Pursuant to the above regulations, any natural person entering or leaving the Community and carrying cash of a value of EUR 10,000.00 or more shall declare that sum using the respective form (CDF), whose sample is laid down by Decree of the MF SR No. 161/2016 Coll. The competent border Customs Office checks the fulfilment of the obligation to declare pursuant to Article II (1) of Regulation No.1889/2005. If the conditions in accordance with the obligation to declare pursuant to Article II (2) of Regulation No. 1889/2005 are not met or if the information provided is incorrect, incomplete or false, the natural person shall be obliged to correct or supplement the data. The border Customs Office shall send the copies of the filled in CDF form and a protocol on the infringement of customs regulations to the FIU SR within the fifth day of the calendar month following the month in which the facts occurred.

However, transportation of cash or transportation of bearer negotiable instruments by postal service or freight transportation was not considered cross-border transportation of cash across external EU borders. Such cases were not subject to the duty of declaration or reporting to competent customs authorities.

The highest volume of cash transported without declaration was detected in 2017 upon entry from Ukraine at Vyšné Nemecké, when a citizen of UA carried EUR 198,736.00, a fine was imposed in the amount of EUR 300.00. In 2018, upon entry at Vyšné Nemecké, EUR 52,299.00, a sanction of EUR 300.00, upon entry at the M.R. Štefánik Airport (a citizen of the U.A.E), EUR 40,309.00, a sanction of EUR 330.00, further, in 2018, two violations of the obligation to declare, one in the amount of EUR 30,945 upon entry at the airport in Bratislava and EUR 30,000.00 upon entry at Veľké Slemence. In the rest of violations, the amount of transported cash was around the limit of EUR 10,000.00.

Cash is captured most frequently at the road crossing point Vyšné Nemecké upon entry and at the international M.R. Štefánik Airport in Bratislava upon entry. Police dogs are also used to detect cash (cash control).

The comprehensiveness of customs procedure for cash is solved in new Regulation No. 1672/2018 of the European Parliament and of the Council, whose most part will come into effect in 6/2021.

Vulnerabilities:

Transportation of cash or transportation of bearer negotiable instruments by postal service or freight transportation was not considered cross-border transportation of cash across external EU borders. Such cases were not subject to the duty of declaration or reporting to competent customs authorities. Customs authorities should improve their knowledge of ML/FT risks and duties and prepare suitable mechanisms to be able to reveal false declarations or failures to file declarations and suspicions of ML or FT. The sanctions imposed in the assessment period for a failure to file a declaration or for an incorrect declaration were not dissuasive.

D. Quality of detection of financial criminal activity

D1. Activity of the Financial Intelligence Unit

The Financial Intelligence Unit (hereinafter the "FIU SR") is a central national unit in the area of prevention and detection of legalisation of proceeds of crime and terrorist financing, and is a coordinator of national money laundering and terrorist financing risk assessment for the assessed period from 2016 to 2019 (hereinafter "NRA II") with the competence for the whole territory of the Slovak Republic.

In a part of the assessment period from 1 January 2016 to 31 August 2019, the FIU SR was an organisational unit of the National Crime Agency of the Presidium of the Police Force (hereinafter "NAKA"). This inclusion of the FIU SR in the structure of the PF raised concerns in assessing the SR by international institutions. Since 1 September 2019, the FIU SR has been an organisational unit of the Presidium of the Police Force, reporting directly to the President of the Police Force of the Slovak Republic. Based on this organisational change, the Director of the FIU SR obtained HR powers and the FIU SR has its own budget item, which are important factors for the development of its activity. The FIU SR prepared underlying data and ensured the organisation of the process of ML/FT assessment of the SR by the Moneyval Committee of the Council of Europe. The legislative framework of the activity of the FIU SR is created by Act No. 297/2008 Coll. on the protection against the legalisation of proceeds of crime and terrorist financing and on the amendment to certain acts as amended (hereinafter "Act No. 297/2008 Coll.") and Act No. 199/2004 Coll., Customs Act and on the amendment to certain acts as amended, according to which the FIU SR receives forms for the declaration of transport of cash, through which persons entering and leaving the EU territory declare cash transportation exceeding the amount of EUR 10,000.00. The FIU SR is also authorised to follow Act No. 171/1993 Coll. on the Police Force as amended. After the organisational changes had been carried out and the Asset Recovery Office had been excluded from the organisational structure of the FIU SR on 1 February 2017 (the number of posts for policemen on the establishment plans was 38), the FIU SR was organisationally divided into four sections:

- Section of Unusual Business Operations,

- Section of Control of Obliged Entities,
- Section of International Cooperation,
- Analytical Section.

The Director is in charge of managing the FIU SR; it should be noted that the Director's position was not occupied in a party of the assessed period from March 2019 to December 2020, and in this period the Director was substituted by the Deputy Director.

Within its competence, the FIU SR is autonomous and independent in performing its powers. Policemen of the FIU SR are admitted to service pursuant to Article 14 of Act No. 73/1998 Coll. on civil service of members of the Police Force, the Slovak Information Service, the Court Guards and Prison Wardens Corps of the Slovak Republic and the Railway Police as amended, which lays down the conditions of competence and procedure of admission to service. The basic requirements imposed on policemen of the FIU SR include integrity, reliability, education specified for the function, health condition, physical condition and psychical condition required for the service. Policemen of the FIU SR are obliged to obtain certificates issued by the National Security Authority and are obliged to keep secrecy as laid down in Act No. 297/2008 Coll. and in Act No. 171/1993 Coll. on the Police Force as amended. No case of violation of integrity by a policeman of the FIU SR was recorded in the assessment period. The FIU SR is a member of the Egmont Group, which is a network of 164 FIUs from around the world; it is also part of the FIU EU platform and part of the grouping of the European FIUs initiated by the European Commission.

In the assessment period from 2016 to 2019, the HR and wage policy at the FIU SR was not at a level corresponding to its importance as an institution with a national competence. Since 1 September 2019, i.e., since the new organisational arrangement of the FIU SR within the Presidium of the Police Force, the FIU SR has had its own budgeted financial resources, for example, for trainings, interpreting and translations, membership fees for international organisations, reimbursement of travel expenses for inland business trips; at the same time, before the FIU SR was detached from NAKA, newer service motor vehicles had been replaced by older ones. The financial remuneration of policemen of the FIU SR is not at an adequate level and it has not changed after the organisational change within the PPF and after the FIU SR had been detached from the NAKA structure. In the assessed period, adequate material and financial resources necessary for its proper operation were available to the FIU SR, however, for the next period, it is necessary to provide the FIU SR with a new comprehensive information system and new service motor vehicles. The comprehensive information system of the FIU SR used within the assessment period was created in 2012 and it needs replacing. The reasons for it include the obsolete hardware and software and insufficient capacity of server disks, as well as the need to keep new data and statistics necessary for international ML/TF measures evaluation of the SR (evaluation by the Moneyval Committee of the Council of Europe, OECD assessment, etc.).

One of the main tasks of the FIU SR is to receive, analyse, process and evaluate UTRs, which the FIU SR receives from obliged entities. Other important tasks of the FIU SR include the control of fulfilment and observance of duties of obliged entities imposed upon obliged entities by Act No. 297/2008 Coll., and international cooperation concerning in particular the

exchange and verification of information necessary to prevent and detect money laundering and terrorist financing. The FIU SR prepares the National Money Laundering and Terrorist Financing Risk Assessment. Customs Offices are obliged to report transportation of cash to the FIU SR (any natural person entering the territory of the SR from a third country (non-EU) or leaving the territory of the SR to a third country and carrying cash of a value of EUR 10,000 or more shall declare that sum in writing to a Customs Authority in a prescribed form, Customs Offices send the forms and notices of a failure to observe the obligation to declare to the FIU SR) pursuant to Article 4 (4) of Act No. 199/2004 Coll., Customs Act and on the amendment to certain acts as amended. To obtain additional information to UTRs from obliged entities, the FIU SR uses in particular the authorisation pursuant to the provision of Article 17 (5) of Act No. 297/2008 Coll. To fulfil its tasks, the FIU SR also actively uses the provision of information by obliged entities pursuant to Article 21 (1) of Act No. 297/2008 Coll. based on which obliged entities provide information and documents on business relations, transactions and persons involved in transactions within a period specified by the FIU SR.

E-mail communication in protected mode, in encrypted form using suitable means /PGP/ with mutually exchanged encryption keys allowing opening the e-mail communication only by the respective addressee is used to receive and forward information in electronic form. Exchange of information at international level is secured by protected communication channels, by user's access rights, passwords and authentication by valid certificates for individual FIUs.

In performing its activity, the FIU SR uses access to records and databases based on which the forwarded information obtains an added value. In its activity, the FIU SR uses access in particular to the following records and databases: Population Register, Register of Motor Vehicles, Centrálna lustračná konzola – CLK (Central Screening Tool) (international matters, INTERPOL, EUROPOL, SIRENE, etc.), Register of Fixed Telephone Lines and Mobile Telephone Numbers, Register of Criminal Prosecution Documents ("DVS"), Register of Legal Persons, Entrepreneurs and Public Authorities with a functionality of Register of Beneficial Owners, Register of Public Sector Partners, Real Estate Register, Commercial Register, Trade Register. At an operational level, the FIU SR actively uses the following internal analytical and administration tools:

- NetReveal (parametric search, visualisation of relations among natural persons, legal persons, criminal records, FIU records, tax records)
- Analyst Notebook (visualisation of chain financial transactions and relationships)
- NetReveal - Analyser (full-text search of FIU records)
- DMS – Daily File Management (administration of documents and files of the FIU SR with a possibility of parametric search).

If an UT analysis shows that there is a suspicion of the criminal offence of legalisation of proceeds of crime, terrorist financing or another criminal offence, the FIU SR will forward information to law enforcement authorities. The FIU SR also forwards information in compliance with Act No. 297/2008 Coll. to other selected institutions – the Police Force for the fulfilment of its tasks pursuant to Act No. 171/1993 Coll. on the Police Force, to the tax administrator and public authorities in the area of taxes, fees and customs, and to public authorities fulfilling tasks of protection of constitutional arrangements, internal order and State security for the fulfilment of their statutory tasks in combating terrorism and organised crime.

The FIU SR forwards information:

- to law enforcement authorities pursuant to Article 26 (2) (b) of Act No. 297/2008 Coll., if the facts suggest that a criminal offence has been committed,
- to the tax administrator and public authorities in the area of taxes, fees and customs pursuant to Article 26 (2) (j) of Act No. 297/2008 Coll., if it justifies the commencement of tax proceedings or is important for the pending tax proceedings unless it endangers the fulfilment of tasks of the FIU SR,
- to PF units for the fulfilment of tasks pursuant to the Act on the Police Force pursuant to Article 26 (2) (l) of Act No. 297/2008 Coll., to public authorities fulfilling tasks of protection of constitutional arrangements, internal order and State security for the fulfilment of their statutory tasks in combating terrorism and organised crime pursuant to Article 26 (3) of Act No. 297/2008 Coll.

Year	2016	2017	2018	2019
Information forwarding by the FIU SR to LEAs	522	354	252	219
Information forwarding by the FIU SR to NAKA	185	223	235	485
Information forwarding by the FIU SR to the Dpt. of Fight Against Terrorism PPF	93	69	65	61
Information forwarding by the FIU SR to RH PF and DH PF	567	419	313	397

Number of UTRs received from banks by the FIU SR:

Year	2016	2017	2018	2019
Number of UTRs received from banks:	2,994	2,496	2,279	2,390
Number of UTRs received from the NBS:	79	59	53	70

Number of UTRs from various obliged entities for the period 2016 – 2019

Obliged entities	2016	2017	2018	2019
Insurance	65	15	14	17
Securities	4	9	6	5
Investment and management companies	48	7	11	5
Exchange offices	5	1	0	13
Payment institutions, electronic money institutions	30	29	21	29
Financial leasing	18	9	9	20

Factoring, forfaiting	0	0	0	1
Financial agent, advisor	0	1	0	0
Casinos, gambling games	15	2	106	14
Real estate agencies	0	0	0	0
Traders in precious metals/precious stones	0	0	0	0
Barristers, notaries public	8	4	4	4
Postal undertaking	22	3	2	1
Auditors / accountants	0	0	0	1

Based on the AML Act, the FIU SR provides information obtained during its activities to the tax administrator and public authorities in the area of taxes, fees and customs if it is important for tax administration and such provision does not endanger the fulfilment of tasks of the Financial Intelligence Unit. In the assessment period, information was sent from the FIU SR centrally to the Financial Directorate of the SR (hereinafter the "FD SR") as follows:

Year:	2016	2017	2018	2019
FD SR	1,361	1,138	980	829
FACO	8	6	12	128

As regards the forwarding of information from the FIU SR to the FD SR it should be noted that the information serves to the tax administrator as underlying data for analytical activities to increase the efficiency of tax audits. Of all information forwarded to the FD SR, 49 % of information was used to open a tax audit (see the part: Exaction of taxes – tab. Use of forwarded information from UTRs by the financial administration for the years 2014-2019). Better tax collection results from such cooperation. Such procedure is in compliance with European Parliament resolution of 26 March 2019 on financial crimes, tax evasion and tax avoidance, in which the European Parliament mentions that improved tax collection in the EU countries will probably lead to reduced crime connected with tax avoidance and money laundering, which follows.

Investigation of criminal activity based on forwarded information from UTRs by the FIU SR to LEAs

Year	UT	Information of the FIU SR	Legalisation of proceeds of crime (Article 233)			Other criminal offences		
			Criminal prosecution	Indictment	Conviction	Criminal prosecution	Charge	Conviction
2016	3,297	498	31	1	0	33	1	0
2017	2,636	354	53	3	0	28	1	1
2018	2,509	252	34	1	0	17	5	0
2019	2 576	219	10	0	0	10	2	0

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL stated in its Report on the 5th round of Mutual Evaluation that:

- the FIU SR receives a reasonable number of UTRs although their quality varies,
- the FIU SR started to improve the feedback given to obliged entities,
- the FIU's dissemination system dissipates its resources into less relevant cases, often not related to ML. This has a negative impact on the quality of the analysis and on the FIU's operational independence. Too many FIU products are sent to the Financial Directorate of SR to be used for tax audit purposes. The FIU SR should reassess the information dissemination system,
- the staff of the FIU SR should be suitably motivated and the FIU SR should have stable and competent management,
- law enforcement authorities insufficiently detect and investigate legalisation of proceeds of crime with respect to suspicions resulting from UTRs,
- supervision authorities should allocate more resources and professional capacities to perform supervision over financial institutions and non-financial institutions and professions, which should be fully risk-oriented,
- at the international level the FIU SR appears to be active and responsive. There are no requests from foreign counterparts which remained unanswered and the feedback provided by the international community regarding the Slovak FIU was generally positive.

Despite the fact that the FIU SR always requires a feedback from LEAs and operational units of the PF regarding the use of sent information, which was obtained from UTRs, the provision of feedback is not at the required level. In this context it should be noted that the request for the provision of feedback from LEAs has been repeatedly discussed by the FIU SR at various levels. Insufficient efficiency in providing feedback from LEAs cannot be justified by sophisticated conduct of perpetrators of legalisation of proceeds of crime with frequent occurrence of an international aspect with the subsequent prolongation of the investigation process.

Money laundering and terrorist financing are international phenomena which can be efficiently prevented and faced at international level only by means of an integrated approach. Therefore, the strengthening and optimisation of international cooperation is a constant priority in various authorities and during bilateral and multilateral consultations between the FIU SR and its international partners.

Overview of numbers of reports on cash transportation from/to the EU received by the FIU SR and the amount of transported cash in 2016 – 2019

Year	Number of reports received	The amount of transported cash in EUR
2016	124	4,016,396.51
2017	152	5,261,245.86

2018	230	8,131,825.21
2019	264	19,625,000.00

International cooperation of the FIU SR

	2016	2017	2018	2019
Foreign requests received by the FIU SR	321	265	240	263
Spontaneous information received from abroad	156	211	420	131
Requests sent by the FIU SR abroad	78	89	85	125
Spontaneous information sent by the FIU SR abroad	321	654	555	502

Vulnerabilities:

- insufficient number of controls of obliged entities performed by the FIU SR, the FIU SR has no risk-oriented procedures which would determine the frequency and intensity of obliged entity controls,
- allocation of resources necessary for the implementation of measures to combat ML/TF is insufficient,
- the information system of the FIU SR is obsolete, it is not sufficiently flexible, there is no systematic solution of collection and processing of information and supporting data for the needs of NRA
- the organisational structure of the FIU SR which was created in 2004 and has not recorded any significant changes, needs to be changed with respect to the development of AML/FT measures and for more efficient fulfilment of tasks (fulfilment of legislative tasks and provision of trainings for obliged entities, NRA preparation, provision of better cooperation with state institutions and private sector),
- insufficient number of posts on the establishment plans at the FIU SR (a partial increase in the number of staff took place in 2019 and in 2021),
- the internal regulation of the FIU SR on the procedure in processing information from UTRs needs to be elaborated in more detail in particular in the part concerning the dissemination of UTRs with the objective to eliminate doubts about autonomous information dissemination.

D.2 Capacities and resources for the detection of criminal activity

The investigators executing the investigation of the criminal offence of legalisation of proceeds of crime and predicate criminal offences are assigned to departments of criminal police of District Headquarters of the Police Force, Regional Headquarters of the /Police Force, the Financial Administration Criminal Office and at the National Crime Agency. Investigators have experience in investigation of predicate criminal offences according to the number of years in service, however, experience in property seizure and financial investigation is insufficient or none, no sufficient attention is paid to this area.

The cooperation of investigators of the PF with the Financial Intelligence Unit consists in particular in receiving information, which the Financial Intelligence Unit obtained from

reports on unusual transactions, based on which criminal prosecution can be commenced under certain circumstances. Additional information important for criminal proceedings is obtained by investigators through legal assistance, through the Interpol National Central Bureau and Sirene National Bureau.

The operational and search activities are carried out without knowledge of the affected person and this also possible to a certain extent (depending on the property) in criminal proceedings. Pursuant to Article 3 of the Code of Criminal Procedure, both the investigator and operational worker may assess the property in respective organisations without knowledge of the owner of the thing. It may be a problem to determine the ownership of financial resources in the cash office of a legal person or to determine movable property (goods, stocks, etc.) because such information can be obtained in particular from accounting or from the employees of the owner of the thing.

Investigators can efficiently cooperate with other domestic and international investigation authorities based on request or legal assistance, i.e., the legal framework for it is in place.

Vulnerabilities:

Financial criminal activities are investigated at departments of criminal police of DH PF and RH PF at investigation units, and at the National Crime Agency. In general, investigators dealing with criminal offences of economic nature have more criminal cases than investigators dealing with criminal offence against property and criminal violence. There are no specialised units for the investigation of money laundering and property seizure.

Trainings in financial investigation for investigators are carried out to a minimum extent; in future, an increased activity in the area of such trainings is expected.

Sufficient technical resources for the fulfilment of "common" tasks are available to investigators. If an unusual thing is to be seized in criminal proceedings (e.g., a great quantity of diesel oil, scrap, cereals, etc.,), the investigator has a problem with storing the seized things. In such case, it is necessary to seize the thing through a support centre; there was a case when the support centre informed that there was lack of financial resources for the transportation and storage of the material, thus, it was not possible to seize the thing. Again, in connection with these cases, the absence of AMO in the assessment period must be pointed out (it is necessary to mention that the proposal for the approval of an act regulating the seized asset management has been withdrawn from the legislative process twice in the past). The Seized Asset Management Office, which was established based on Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts, should start its activities on 1 August 2021.

Obviously, financial intelligence services are not used sufficiently in pending criminal proceedings. Investigators also consider the provision of legal assistance from certain countries to be time-consuming. There is no statistics concerning the number of investigators involved in the process of property seizure.

Within the reorganisation of the PPF in 2021, particular emphasis will be given to the support and development of analytical activities focused on the detection of the most complex schemes of serious criminal offence of economic nature concerning corruption. Assignment of the service of financial police to the Presidium of the PF with the creation of suitable structures

for the initiation of the mechanisms of financial investigation, detection and seizure of proceeds of crime will be important.

D3. Integrity and independence of investigators of financial criminal activity

The criminal activity of investigators of financial criminal activities is at a level showing no significant year-on-year changes. No negative influence on investigators in connection with investigation of ML and property seizure was detected. The area of seized asset management and insufficient seizure of assets remains problematic; however, this is not caused by influence of other persons on the investigator, the reason is the insufficient use of financial investigation and legislative limitations in the area of asset seizure.

Investigation takes place without interventions, political or social pressure, corruption, intimidation or abuse of position and asset seizure takes place without undesirable external interventions. Investigators are procedurally independent by law. Pursuant to the Code of Criminal Procedure, only prosecutors supervise the lawfulness in pre-trial proceedings and in the proceedings prior to the commencement of criminal prosecution. Statistics on criminal activities of investigators in executing cases of ML/asset seizure in general do not show a high rate of criminal activity in connection with corrupt behaviour in the area of ML and asset seizure.

D4. Efficiency of international cooperation

The Slovak Republic has a sufficient legal framework for the provision and requesting of legal assistance from abroad. The length of request handling by foreign state authorities is the only obvious deficiency. The SR provides legal assistance within the shorted time possible. Cooperation in the area of legal assistance is covered by the GPO SR, which coordinates and supervises proper and timely request handling. Police units provide international cooperation at the requested level except for cooperation with certain countries where there are delays in the process.

Quick responses to requests for legal assistance to be provided by investigators are supervised by prosecutors, who, if necessary, efficiently coordinate the work of investigators so that responses are provided properly and in time. The Slovak Republic can provide legal assistance at the request for cooperation based on proceedings without previous conviction and related preliminary measures. It also uses international law enforcement networks for information sharing (Interpol, SIRENE, FIUs, etc.). Information exchange is also provided through joint contact points and through seconded police officers.

On request, the SR will provide legal assistance urgently; legal assistance is also provided based on a request regardless of whether the perpetrator has been convicted of a criminal offence abroad or not.

The police have a legal mandate authorising them to exchange information with foreign partner authorities. Limitations of information provision are adequate to the circumstances and to areas, from which information is requested. Information is provided bilaterally in compliance with law.

Vulnerability:

Time needed to deal with a request sent within legal assistance and through Interpol from abroad is relatively long.

D5. Availability of reliable information and evidence

D5.1 Level of economy formalisation

Key determinants of the size of shadow economy include the quality of regulation, efficiency of the Government and human capital. A comprehensive package of reforms focused on the driving forces of individual countries is necessary for the successful fight against shadow economy. The list of policies, which are most important for the developing economies of Europe, includes: reducing the regulatory and administrative load, support of transparency and improvement efficiency of the Government, as well as improvement of tax regulations, automation of procedures and support of electronic payments.

Shadow economies persist for various reasons. Employees and companies may opt for informality in order to avoid taxes and pensions or social security payments or labour market regulations. However, in some cases, shadow economy may serve as a source of employment and income in the absence of opportunities in the formal sector or as a security network during cyclical decrease. Thus, shadow economy may contribute to the overall growth.

Based on data for the previous six years, in Slovakia, the average volume of shadow economy was at a level of 13.4 % of GDP. In comparison, Austria reaches an average value of this parameter of 7.29 % and Germany 10.38 %. Achieving a zero share of shadow economy is not feasible; zero unemployment is not feasible either. However, if Slovakia managed to reduce shadow economy to a level of Austria, the state budget would obtain over EUR 1.78 bn. in taxes and levies. The tax and regulatory burdens are the most essential factors encouraging shadow economy.

Slovakia has a complicated and opaque tax system. With a correct adjustment of measures, Slovakia could jump to a lower level of shadow economy. The area of VAT collection is another area promising benefit for the state budget. The European Economy calculated a total VAT loss in European Union States for 2017 of EUR 137 bn. The SR essentially lags in this parameter. According to tax experts, the last measured gap between the expected income and real VAT collection reached 22 %. The downward trend is positive; however, the decrease is too slow to get the SR closer to States with more efficient control of VAT collection. Such States include Austria (8%), Germany (9 %), but in particular Slovenia (0%).

"It is necessary to appreciate the effort of the Financial Administration, which speaks about the success of tax controls reaching 75 % and about plus values in additional collection of taxes and fight against frauds in the amount of EUR 3.7 bn. in the previous years. It should also be appreciated that the Financial Administration has already started working on automatic identification of suspicious companies and on the concentration of control capacities on these

companies. However, the SR misses the resulting easement for honest companies fulfilling their duties on a regular basis."

Size of shadow economy in the SR compared to other countries:

Country / Year	2016	2017	2018	2019	Ø 2014-19
Austria	7.8	7.1	6.7	6.1	7.29
Czech Republic	14.9	14.1	13.6	13.1	14.35
Germany	10.8	10.4	9.7	8.5	10.38
Hungary	22.2	22.4	22.7	23.2	22.34
Poland	23.0	22.2	21.7	20.7	22.40
Slovakia	13.7	13.0	12.8	12.2	13.40

D5.2 Reliability of financial records and books

The reliability of accounting records/books assesses whether legalisation investigators can rely on financial records/books to track the flows of financial proceeds of crime in the cases of legalisation of proceeds of crime. The reliability of financial records/books is affected by the level of financial integrity, efficiency of exaction of taxes and availability of independent audit.

Not always, investigators can rely on financial records from enterprises to be able to track cash flow in investigating the cases of legalisation. Information provided by the banking sector is reliable; however, a problem with tracking the flow of financial resources occurs when cash is withdrawn. It is difficult to find out how financial resources were disposed of according to accounting records of legal persons due to inconsistent book-keeping by entities committing criminal activities.

D5.2.1 Level of financial integrity

LEAs have access to information from public authorities in the area of taxes, fees and customs by submitting a request within legal rules (Code of Criminal Procedure, Act on the Police Force).

In investigating criminal offences of economic nature, investigators cannot rely on the cooperation of individual enterprises when obtaining financial records necessary to track cash flow. Some business companies usually do not provide collaboration in investigating and often they cannot be contacted and their accounting records cannot be obtained.

Vulnerabilities: Not always, investigators can rely on financial records from natural and legal persons having the reporting duty in accordance with applicable legal regulations in order to monitor cash flow in investigating the legalisation. Information provided by the banking sector is reliable; however, a problem with tracking the flow of financial resources occurs when cash is withdrawn. It is difficult to find out how financial resources were disposed of according to accounting records of legal persons due to inconsistent book-keeping by entities committing criminal activities.

D5.2.2 Efficiency of exaction of taxes

The tasks of the Financial Administration and its individual authorities are laid down by Act No. 35/2019 Coll. on the Financial Administration and on the amendment to certain acts as amended, i.e., to protect the fiscal and commercial policy interests of the Slovak Republic and European Union and to fulfil tasks in protecting the internal market of the European Union. The Financial Administration cooperates with international organisations, tax administrations and customs administrations of other States to an extent and under the conditions laid down by legally binding acts of the European Union, international treaties or agreements among the participating parties.

The main mission of the Financial Administration is to ensure uniform tax and customs duties collection to a full amount of claim of the SR and EU, to ensure protection of economic interests, commercial policy measures and security interests of the State and EU. The Financial Administration fulfils the tasks resulting from the respective legislation, in particular in preventing the violation of tax and customs regulations, in the area of direct taxes and fees pursuant to special regulations, in supervising the observance of generally binding legal regulations, EU regulations and international treaties ensuring the implementation of tax policy, customs policy, business policy, security policy and agricultural policy, during goods circulation in contact with third countries. It performs customs supervision of goods within the single customs territory of the EU, in the area of administration of indirect taxes, tax supervision of goods subject to tax administration, provides for mutual international assistance and cooperation in tax and customs duty administration and in recovering financial receivables. It fulfils tasks in the area of customs tariffs, customs duty rates, customs value, tariff classification of goods, origin of goods, statistics of trade with third countries and statistics of trade among EU Member States, and fulfils other tasks laid down by special regulations.

The priority task of the Financial Administration is to ensure the fulfilment of the income part of the state budget and EU budget. The state budget is the basic instrument of the State's financial policy ensuring the division of the State's resources. The key task of the Financial Administration is to fulfil the statutory amount of income of the state budget, monitor the fulfilment of income and adopt measures to achieve its fulfilment by collecting efficiently the tax and customs duty income. It is important to focus on the prevention in collecting tax and customs duty and on the support of voluntary fulfilment of state budget income, to estimate the occurrence of tax and customs duty arrears of tax and customs duty debtors, to support the implementation of tax liability simulation based on a behavioural analysis of economic behaviour, to detect delinquencies and adopt efficient measures for successful collection of taxes and customs duties.

Within the tax framework, in accordance with Act No. 563/2009 Coll. on the administration of taxes and fees and on changes in the system of territorial financial authorities as amended (Tax Procedure Code), the Financial Administration has the following authorisations:

- Search for unregistered tax entities

- Local screening – looking for evidence, verifying and finding the facts necessary for the purposes of tax administration
- Seizure of a thing – necessary to prove the facts in tax administration with the possibility of forfeiture of a thing
- Request for data for the purposes of tax administration in accordance with Article 26
- Tax audit – finding or verifying the facts decisive for tax assessment or observance of provisions of special regulations
- Execution proceedings.

Taxes are perceived as the means to fill the State Treasury, from which goods beneficial to the whole society are settled. Equality is the principle applied in tax collection and in subsequent tax execution, if any. Equality means that everybody has the same rights in the same case assumed by law, as well as that everybody has the same duties. In this context, tax execution can be perceived not only as an auxiliary tool or means but even as the duty of the State to ensure equality, equal treatment of all obliged entities. In consequence, it is obvious that tax execution is not, and should not be perceived in the rule of law, as the objective or purpose of tax payment process because the tax collection itself is not the objective; rather, it is the means leading to satisfaction of the citizens. The State is not interested in the highest possible number of tax executions.

Ensuring the enforcement is an important element of the whole problem of legalisation. It means not only tax execution but also real achievement of return/reimbursement of the harm caused. Knowledge of property transfers should be used for legal guarantees of proper procedure, which would allow full application of unenforceable or invalid legal actions.

Currently, the FD SR ensures a high-quality analytical support for the whole area of tax administration. Nor this support, however, can be considered an efficient tool because data sources are limited to a great extent by the competence possibilities of the Financial Administration.

TAX AUDIT

As regards the performance of tax audits or control activities as such, they can be divided into

- preventive
- repressive.

The system of criteria of selection of tax entities for audit is based on the risk rate, with the determination of a maximum number of tax entities per individual tax authority per year. All the units as well as tax authorities are involved; tax authorities submit suggestions to the Financial Directorate department in charge in the form of proposals, and after the analysis is performed by the department, the proposals are included in the list of audits or if necessary, the reasons for proposals are consulted with tax authorities.

The objective is, in the interest of increasing the efficiency of control activity and implementation of measures for suppressing and preventing criminality in the area of value

added tax and other taxes, and based of the identification of risky behaviour of tax entities from the outputs of analytical systems and other available data with the objective to achieve real protection of the State's interests and optimisation of work load of controllers of tax authorities, to exactly specify a duty for individual departments and authorities of the Financial Administration (including the department of internal control and inspection, etc.) to submit, in the event that a necessary performance of tax administration acts by tax authorities is identified, proposals for their performance to the Department of Risk Analysis and Management. An internal regulation ensures and sets systematic continuous cooperation (periods, the way how to submit requests, how to respond, etc.) with all departments and bodies of the Financial Administration. Besides the number, also efficiency indicators are set by the plan of audit activities. The indicator of efficiency of audit is set on the basis of reached efficiency values in the previous period taking into account the current approach to control activity planning so that it reflects the possibilities of the tax authority. It is calculated as the quotient of the number of audits performed with a finding and the total number of audits performed. Limits are specified for a minimum amount of finding when an audit is considered efficient.

Within the scope of improvement of control activity efficiency (performance of audits and local screenings), it should be ensured that future plans of audits adequately cover all main types of taxes and main segments of tax payers, including the well-off persons. At the same time, it is necessary to ensure the analysis of a tax entity from all points of view – which assumes a broader spectrum of information (for that, data from various sources need to be integrated) for an integrated view of the tax entity (because the entity's behaviour concerning the detected tax is risky rather than the tax as such) so that control activity performance is focused on the verification of all types of taxes ensuring a pro-customer approach, by verifying all the facts (within all taxes) by one input, as well as to improve controllers' knowledge in terms of use of a broader spectrum of methodologies of indirect control *(in necessary, accompanied by an amendment to legislation*) and detection of legalisation of proceeds of crime.

The prepared summary and the statistics relating to the efficiency of control activities of the Financial Administration, as well as the statistics of recorded criminal complaints filed by the Financial Administration for 2013 - 2017 according to individual types of tax criminal offences in relation to the number of tax audits performed, in which information from unusual transactions were used, imply a positive influence on the detection of tax criminality.

Table: Use of information from unusual transactions by the Financial Administration in 2016–2019

Year	Pieces of information received from the FIU SR	Out of it, the number of pieces of information from the FIU SR which affected the risk profile of the entity at the beginning of a tax audit	Share of information from the FIU SR which affected the risk profile of the entity at the beginning of a tax audit
2016	1,255	701	56%
2017	1,097	561	51%
2018	927	448	48%
2019	681	218	32%

Table: Number of registered criminal complaints lodged by the Financial Administration in 2015-2019 by individual types of tax criminal offences

Criminal complaints sent by the Financial Administration	2016		2017	
	Number of criminal complaints lodged by the FD	Reported loss in EUR	Number of criminal complaints lodged by the FD	Reported loss in EUR
of the Criminal Code Article 276 of the Criminal Code	416	180,709,942.38	659	136,489,978.13
Failure to pay tax and insurance premium Article 277 of the Criminal Code	80	2,081,186.18	107	980,907.41
Tax fraud Article 277a of the Criminal Code	140	6,592,768.64	191	7,427,342.83
Failure to pay tax and insurance premium Article 278 of the Criminal Code	322	21,419,152.03	209	9,998,831.65
Obstructing the execution of tax administration Article 278a of the Criminal Code	3	0.00	5	0.00
Distortion of data in financial and commercial records Articles 259, 260 of the Criminal Code	12	0.00	5	0.00
Total	973	210,803,049.23	1176	154,897,060.02

Criminal complaints sent by the Financial Administration	2-12/2018		2019	
	Number of criminal complaints lodged by the FD	Reported loss in EUR	Number of criminal complaints lodged by the FD	Reported loss in EUR
Tax and insurance premium evasion Article 276 of the Criminal Code	315	61,438,131.56	267	45,098,440.97
Failure to pay tax and insurance premium Article 277 of the Criminal Code	31	897,768.13	132	6,162,579.03

Tax fraud Article 277a of the Criminal Code	70	3,883,128.65	67	7,194,851.92
Failure to pay tax and insurance premium Article 278 of the Criminal Code	178	4,582,002.95	628	16,348,743.81
Obstructing the execution of tax administration Article 278a of the Criminal Code	25		8	
Distortion of data in financial and commercial records Articles 259, 260 of the Criminal Code	25		8	
Other criminal offences, e.g., Article 221, Article 225	34	1,210,602.14	10	417,838.94
Total	678	72,011,633.43	1,120	75,222,454.67

EDUCATION OF FINANCIAL ADMINISTRATION EMPLOYEES

Tax controllers usually have 2nd degree university education, however, mostly focused on economics; there are few lawyers among them. No rotation is prescribed for controllers.

The objective of the system of education in the conditions of the Financial Administration is to obtain education by Financial Administration members and employees, to improve and deepen the qualification for the performance of expert and specialised activities.

Education types:

- adaptation – a systematic, organised, evaluated educational process with the objective to facilitate the adaptation of new Financial Administration members and employees and to ensure that they acquire, develop and use their professional and personal potential necessary for civil service and work performance
- professional:
    - basic – taking a basic course and passing a lower exam, i.e. proving theoretical knowledge and solving a practical task before the examination commission, which is a qualification precondition to hold a position and for the assignment to permanent civil service,
    - expert – taking an expert course and passing a higher exam, i.e. the application of theoretical knowledge and practical skills in solving a case study before the examination commission, which also is a qualification precondition
- competence-related – systematic deepening of qualification of Financial Administration members and employees with the objective of continuous maintenance, renewal, improvement and supplementation of knowledge, skills, abilities and habits for civil

service performance for individual positions according to the character of performed service activities and for the performance of work agreed ion the contract of employment; it consists of professional competence education, personal development, training of Financial Administration members, service cynology, IT education, language education, etc.

Forms of education and their characteristics:

- *attendance form*, mass, group and individual:

  Mass forms – intended for a greater group of participants:

  - trainings – a short-term form of educational activity whose objective is to obtain or update knowledge;
  - conference – an event with a selected topic focusing on expressing opinions on various aspects of the professional area;

  Group forms:

  - course – an independent educational form consisting of one or several teaching modules with contents selected and structured according to the respective educational project,
  - seminar – the objective is to strengthen and expand the already obtained knowledge and skills of one or several teaching subjects or topics related to performance of civil service or work
  - workshop – the objective is to strengthen and expand the already obtained knowledge and acquire new practical skills in solving practical examples, case studies through interactive cooperation between the lecturer and educational activity participant
  - training – a practically oriented form of education whose objective is the comprehensive development of already obtained knowledge, practical skills, abilities and habits leading to comprehensive performance of civil service and work

  Individual forms:

  - mentoring – a method of mutual cooperation between the mentor/superior and a new Financial Administration member or employee with the objective to hand over necessary information, work experience and skills to a new Financial Administration member or employee and consult with them draft solutions for the best possible adaptation in the environment of the Financial Administration
  - coaching – the objective is to support the development of skills and abilities of Financial Administration members or employees, usually by superiors; based on the obtained experience, they help Financial Administration members or employees transform their knowledge into skills and develop their potential in order to maximise their performance

- *distance form*, e-learning and webinar
- *self-study* – a continuous process of acquiring and expanding knowledge, skills, abilities, habits and experience, which is carried out by Financial Administration

members or employees separately and independently from the educational activities provided by the Academy of the Financial Administration;

- *internship* – professional practice of a Financial Administration member or employee at a specified organisational unit within the Financial Administration in a specified time period determined by the superior of the sent Financial Administration member or employee, based on an agreement with the superior of the respective organisational unit of the Financial Administration; the purpose is to apply theoretical knowledge in practice, to acquire and improve practical abilities and skills;
- a combination of the above forms.

Verification and evaluation of knowledge and end of education: verification is carried out in written or oral form, as a test or a practical exam, e.g. by solving case studies:

- the result of the exam can be:
  - partial – passed/failed
  - general – for a course and when taking a lower exam, higher exam, final exam, during adaptation education: passed/failed; for other educational activities taken/not taken

- completion may be:
  - regular – taking an educational activity within the scope specified in the educational project;
  - premature – if a Financial Administration member ends the study only for provable health or family reasons based on a written request for a premature end of the study;
  - exclusion from the study – if duties connected with the study of Financial Administration members are not observed

Statistics of cases of violation of tax authority integrity (in particular by employees performing tax audits). The main task in the area of internal control within the Financial Administration was to refer to failures to observe and violations of generally binding legal regulations and internal acts by Financial Administration members, both armed and unarmed, thus contributing to improvement of lawfulness in customs and tax procedures including preventive activities.

Internal control activities

Number of controls commenced per year		Scheduled/ combined controls completed		Unscheduled controls completed		Total uncompleted controls
		a protocol/report	a record	a protocol/report	a record	
2016	62	41	14	1	2	4
2017	60	48	10	1	0	1
2018	68	29	18	16	2	3

2019	64	41	8	12	0	3
TOTAL	254	159	50	30	4	11

COMPLAINTS	Year				TOTAL
	2016	2017	2018	2019	
Total number of complaints	412	417	282	287	1398
Complaints pending as at 31 Dec.	52	31	29	36	148
Complaints concluded as at 31 Dec.	360	386	253	251	1250
- forwarded	52	79	51	52	234
- postponed	167	118	80	72	437
- examined	141	189	122	127	579
- out of the examined, justified	24	47			71

Inspection

	Year				TOTAL
	2016	2017	2018	2019	
Verified suggestions from legal persons, natural persons and other general government authorities	58	70	63	23	214
Verified suggestions resulting from internal search activities	52	61	44	21	178
Violations of discipline	33	23	20	9	85
Verifications in internal and external applications	4943	6211	3781	3130	18065
Number of accused person from the Financial Administration	2	12	3	1	18
Forwarded notices of suspicions of criminal offence to LEAs		26	6	16	48
Breathalyser tests		176	87	199	462
Of which positive		2	5	4	11

INDEXES OF PERCEPTION AND SURVEYS OF LEVEL OF CORRUPTION/INTEGRITY OF TAX AUTHORITIES

A qualitative survey of perception of satisfaction with the Financial Administration of the SR was carried out in April 2015, in the area of use of services of the Financial Administration (as regards frequency, 36% of respondents use the services frequently and 41% of respondents occasionally), satisfaction with them (60%), as well as evaluation of planned steps and changes in the Financial Administration (71% of respondents have not noticed any changes, and 18 % of respondents have noticed positive changes).

SYSTEM OF SANCTIONS

In the Slovak conditions, subsequent State interventions in the form of negative material situation of tax entities still prevail, starting from imposition of various sanctions and ending by criminal consequences of tax liability application.

In the fight against the abuse of tax system, various motivation schemes have a certain importance so that tax entities do not act at all, or to contribute to the elimination of negative consequences of behaviour. A strategy concerning the support of voluntary fulfilment of tax liabilities in the form of soft warning messages – notices for tax entities sent by the Financial Administration regarding fulfilment of tax liabilities – is carried out in the area of tax administration performance, including:

- Notices of the existence of arrears on the taxpayer's personal account are sent on a monthly basis after the closing of books
- Reminding the deadline to entities with an extended period for individual income tax return submission
- Notices of unpaid prescribed advance tax for individual income tax are sent on a quarterly basis
- Notices of special tax regimes on an annual basis
- Notices of a failure to submit corporate income tax on an annual basis
- Notices of the correct way of storage of accounting documents, in particular Annual Reports, in the Registry of Financial Statements, to eliminate the incorrectly filed accounting documents and Annual Reports, which cannot be forwarded to the Registry of Financial Statements on an annual basis
- Notices of turnover amount for the purpose of VAT and change of taxation period
- Notices to accounting units which failed to save their financial statements in the Registry of Financial Statements (hereinafter the "RFS")/ a notice requesting the fulfilment of this duty
- Notices of discrepancies in the data reported in control statements and in VAT returns
- Tax entities welcome the sending of friendly notices by the Financial Administration.
- Notices to entrepreneurs of the duty to use eKasa Klient cash registers for the registration of revenues received in cash. SoWa was sent during the implementation of the eKasa system, i.e., from 03/2019 to 07/2019. The evaluation of the SoWa measure is not available due to its nature and focus. The objective was to submit information to entrepreneurs on the duty to procure an eKasa Klient cash register by the deadline set by law (1 July 2019) and use it in recording revenues (note: a suspension of the duty to use the eKasa Klient cash register was approved immediately before the eKasa system rollout in June 2019, therefore, the SoWa content was focused on meeting the duty to apply for the assignment of a code for eKasa Klient cash register and on using it from 1 July 2019).

Sanction measures are in the form of sanctions imposed as tax legal sanctions for illicit conduct of tax entities. The performance of tax administration for the area of imposition of sanctions is governed by Act No. 563/2009 Coll. on the administration of taxes and fees and on

changes in the system of territorial financial authorities as amended (Tax Procedure Code), which specifies the violations, for which s sanction can be imposed:

- Article 154 Administrative Delinquencies (unlawful conduct committed by the person who fails to fulfil a tax liability of monetary or non-monetary nature in a correct amount or period within the time-limit according to the Tax Procedure Code or a special act)
- Article 155 Fines (a sanction imposed by the tax administrator for a fact found, which is an administrative delinquency of non-monetary nature, such as a failure to file a tax return pursuant to the Tax Procedure Code or a special act, e.g., Act No. 222/2004 Coll. as amended, a failure to fulfil the registration duty, a failure to fulfil the duty in performing tax audit, etc.)
- Article155a Aggregate Fines (one fine for the commission of several administrative delinquencies)
- Article 156 Interest on Late Payment (a sanction imposed by the tax administrator for a failure to pay the tax amount or to pay tax by the deadline).

Act No. 394/2012 Coll. on limitation of cash payments has been in effect in the SR since 1 January 2013; based on it, cash payments are prohibited if the amount paid exceeds EUR 15,000.00 between natural persons-non-entrepreneurs, and cash payments are prohibited if the amount paid exceeds EUR 5,000.00 between business entities. Pursuant to Act No. 394/2012 Coll. on limitation of cash payments, a delinquency is committed by a person who

a) as the transferring person, violates the ban on handing over a cash payment amounting to EUR 15,000.00/ EUR 5,000.00 or

b) as the recipient, violates the ban on accepting a cash payment amounting to EUR 15,000.00/ EUR 5,000.00

If a cash payment in an amount exceeding EUR 5,000.00 is made by a legal person or a natural person-entrepreneur, they commit an administrative delinquency pursuant to Article 10 of Act No. 394/2012 Coll. on limitation of cash payments. The assessment of delinquencies and administrative delinquencies pursuant to Act No. 394/2012 Coll. on limitation of cash payments for the period 2016 to 2020 is provided in the following tables:

Number of cases:

Customs Office	2,016	2,017	2,018	2,019	2,020	Sum total
Customs Office Banská Bystrica	2		1			3
Customs Office Bratislava			2			2
Customs Office Košice	2		1			3
Customs Office Michalovce	14	7	7	6		34
Customs Office Nitra			14	20	29	63
Customs Office Prešov	1	1		1		3

Customs Office Trenčín	2	5	1	3	7	18
Customs Office Trnava				2		2
Customs Office Žilina				65	24	89
Sum total	21	13	26	97	60	217

Amount of fine:

Customs Office	2,016	2,017	2,018	2,019	2,020	Sum total
Customs Office Banská Bystrica	€100		€100			€200
Customs Office Bratislava			€30			€ 30
Customs Office Košice	€1200		€150			€1350
Customs Office Michalovce	€1600	€400	€140	€270		€2410
Customs Office Nitra			€330	€128	€180	€638
Customs Office Prešov	€0	€300		€50		€350
Customs Office Trenčín	€600	€530	€250	€100	€120	€1600
Customs Office Trnava				€310		€310
Customs Office Žilina				€4240	€1655	€5895
Sum total	€3500	€1230	€1000	€5098	€1955	€12,783

Infringement of Act No. 394/2012 Coll. – **number of cases**	2,015	2,016	2,017	2,018	2,019	2,020	Sum total
Delinquency	9	10	8	2	73	30	132
Administrative delinquency	7	9	5	10	6	4	41
Sum total	16	19	13	12	79	34	173

Infringement of Act No. 394/2012 Coll. – **amount of fine**	2,015	2,016	2,017	2,018	2,019	2,020	Sum total
Delinquency	€2,368	€1,330	€650	€60	€4,472	€2,395	€11,275
Administrative delinquency	€12,440	€2,170	€580	€1,040	€720	€610	€17,560
Sum total	€14,808	€3,500	€1,230	€1,100	€5,192	€3,005	€28,835

Vulnerability:

According to the above findings, the fines imposed do not have a sufficient dissuasive effect taking into account the authorisation of customs or tax authorities to impose a penalty for a delinquency up to an amount of EUR 10,000.00 or for an administrative delinquency up to an amount of EUR 150,000.00 pursuant to Act No. 394/2012 Coll. on limitation of cash payments.

D5.2.3 Availability of independent audit

The purpose of the audit of financial statements is to allow the auditor to express an opinion whether the financial statements have been prepared, in all material respects, in compliance with the set financial reporting framework. The auditor also has to follow the Code of Ethics for Auditors. Auditors perform audit in compliance with the International Standards on Auditing –ISA.

In general, auditing can be characterised as a separate specific profession focused on multiple examination and integral qualified evaluation of an enterprise as a dynamic object, with an unambiguous conclusion in terms of the purpose for which it is ordered. The purpose is formulated by the customer, and the auditor undertakes to provide them with qualified (professional) conclusions for decision-making. Based on the above definition it can be stated that the basic objective of audit is to improve the credibility of accounting information of the companies obliged to publish financial statements and Annual Reports and to have the financial statements verified by an auditor. The secondary (derived) objective of the audit is its moral and preventive effect against the occurrence of errors and frauds.

Auditor's independence concept

To fulfil the objectives of audit, financial information user must perceive the auditor as an independent person. Thus, the term independence must be understood:

- as independence in relation to examined auditing, accounting and other information,
- as independence in relation to those preparing the information,
- as independence in relation to those using the information for decision-making.

The concept of independence in the legislation of the Slovak Republic is concentrated in the wording of Article 21 of Act No. 423/2015 Coll. on statutory audit laying down that "In performing statutory audit, the statutory auditor and audit firm are impartial and independent from the audited entity or customer. The statutory auditor and audit firm must not perform statutory audit in the audited entity if they take part in its decision-making processes and are not independent from it."

In acting in the public interest, the auditor should follow ethical requirements defined in the Code of Ethics for Auditors and to observe it. The Code of Ethics for Auditors determines the main ethical principles followed by auditors. It also specifies basic ethical principles, their possible threats and measures to be taken by an auditor to prevent them. The Code of Ethics for Auditors determines minimum principles to be observed by the member organisations of IFAC (International Federation of Accountants) unless the legislation of the respective country regulates some area otherwise.

Based on Act No. 423/2015 Coll. on statutory audit and on the amendment to Act No. 431/2002 Coll. on accounting as amended (hereinafter "Act No. 423/2015 Coll."), the Audit Supervisory Authority has had the competence to perform reviews of statutory audit quality pursuant to Article 35 of Act No. 423/2015 Coll. since 17 June 2016.

The Slovak Chamber of Auditors has issued a Code of Ethics for Auditors consisting of two parts. The first part is the document explaining in more detail the application of the Code of Ethics for Auditors in the conditions of the legislation of the SR. The second part is an official translation of the International Code of Ethics for Professional Accountants along with International Independence Standards issued by the International Ethics Standards Board for Accountants IESBA at the International Federation of Accountants IFAC, which was issued in 2018.

D 5.3 Customer due diligence framework quality

D 5.3.1 Availability of reliable identification infrastructure

In performing customer due diligence, the obliged entities use the on-line access to the databases of stolen identity cards and passports based on which they verify on-line the authenticity of the submitted document.

Irregular SVK documents detected at the external borders within the EU and at the internal air borders:

Y2016 – 365 SVK documents, 258 individuals

Passport – 41, ID card – 38, Residence permit – 2, Visa – 4, Other – 17, Crossing stamps - 263

The way of forgery: 316 false, 16 impostors (a genuine document abused by another person), 16 unspecified method, 7 replacement of a whole data page, 4 modifications on the data page, 2 altered, 2 photo replaced

Y2017 – 306 SVK documents, 227 individuals

Passport – 41, ID card – 64, Residence permit – 2, Visa – 2, Other – 11, Crossing stamps – 186

The way of forgery: 254 false, 18 unspecified method, 11 impostor, 8 altered, 5 replacement of a whole data page, 4 photo replaced, 3 modifications on the data page, 2 a genuine document acquired fraudulently, 1 illicit intervention

The genuine documents acquired fraudulently - SVK visas:

SVK visas found: 1 UKR at Budomierz (Poland) and 1 GEO at NYO (Stockholm Skavsta Airport in Sweden)

Y2018 – 409 SVK documents, 350 individuals

Passport – 65, ID card – 186, Residence permit – 0, Visa – 2, Other – 10, Crossing stamps – 146

The way of forgery: 322 false, 44 unspecified method, 22 impostor, 2 altered, 4 replacement of a whole data page, 4 photo replaced, 8 modifications on the data page, 2 genuine documents acquired fraudulently, 1 modification on the data page, 1 illicit intervention

The genuine document acquired fraudulently - SVK passports and SVK ID cards:

SVK passport found: 1 IRN at PMI (Palma de Mallorca Airport in Spain), and SVK ID cards found: 1 PAK at SNN (Shannon Airport in Ireland)

Y2019 – 450 SVK documents, 366 individuals

Passport – 112, ID card – 221, Residence permit – 3, Visa – 8, Other – 33, Crossing stamps – 73

The way of forgery: 340 false, 61 unspecified method, 23 impostor, 9 altered, 6 replacement of a whole data page, 3 photo replaced, 4 modifications on the data page, 2 stolen clean copies, 1 replacement of other than data page, 1 illicit intervention

Stolen clean copies of SVK ID cards:

SVK ID card found: 1 RKS at Evzoni (Greece) and SVK ID card found: 1 BIH at Obrezhje (Slovenia)

D5.3.2 Availability of independent information sources

Obliged entities use a great scope of independent information sources:

- Commercial Register of the SR and Trade Register of the SR, Register of Non-Governmental Non-Profit Organisations, Registry of Financial Statements – a general government information system,
- information on beneficial owners – Register of Legal Persons, Entrepreneurs and Public Authorities, Register of Public Sector Partners,
- Central Register of Outstanding Receivables of the State – the register publishes the persons towards whom the Slovak Republic records outstanding receivables which came into existence after 1 January 2014, and which are covered by Act No. 374/2014 Coll. on the outstanding receivables of the State and on the amendment to certain acts as amended,
- information from the credit register available to banks,
- information from the Social Insurance Agency,
- information from the Real Estate Register,
- information on the customer from history (account statements, previous applications for bank products, the existing products provided, “black” and “grey” lists, questionnaires concerning the bank products provided, KYC questionnaires before a business relationship is established and during a business relationship, etc.),
- information on economic results of business entities, such as www.finstat.sk.

5.3.3. Availability of and access to information on beneficial ownership

System of information on beneficial owners in the SR is based on mechanisms and principles contained in several acts:

- Act No. 297/2008 Coll. on the protection against the legalisation of proceeds of crime and terrorist financing and on the amendment to certain acts,

- Act No. 315/2016 Coll. on the Register of Public Sector Partners, effective from 1 February 2017,

- Act No. 272/2015 Coll. on the Register of Legal Persons, Entrepreneurs and Public Authorities and on the amendment to certain acts,

- Act No. 346/2018 Coll. on the Register of Non-Governmental Non-Profit Organisations and on the amendment to certain acts,
- Act No. 530/2003 Coll. on Commercial Register and on the amendment to certain acts as amended,

Since 1 November 2018, the legal persons registered in the Commercial Register, which are not general government entities or issuers of securities admitted to trading on a regulated market, non-investment funds, non-profit organisations providing welfare services and foundations, have been obliged to register in non-public parts of respective source registers (the Commercial Register, Register of Non-Investment Funds, Register of Non-Profit Organisations Providing Welfare Services, Register of Foundations) the data on their beneficial owners. The following data on beneficial owners is recorded in the source registers: name, surname, personal number or date of birth if no personal number has been assigned, permanent address or other residence address, nationality, and type and number of ID card or a circle of persons considered the beneficial owner, and data establishing the position of beneficial owner. The data on beneficial owners recorded beneficial owners beneficial owners beneficial owners were not publicly available.

The data on beneficial owners from the respective source registers are provided to the central register – the Register of Legal Persons, Entrepreneurs and Public Authorities - kept by the Statistical Office of the Slovak Republic. The Statistical Office of the SR provides a remote, continuous and direct access to the data on beneficial owners to government institutions pursuant to Article 7a (2) of Act No. 272/2015 Coll. on the Register of Legal Persons, Entrepreneurs and Public Authorities and on the amendment to certain acts as amended (FIU SR, Ministry of Finance of the Slovak Republic, National Bank of Slovakia, National Security Authority, courts, Tax Authority, Customs Office, etc.) and to obliged entities for the fulfilment of their tasks in performing customer due diligence.

The legal persons registered in the Commercial Register, non-investment funds, non-profit organisations providing welfare services and foundations, which were established before 31 October 2018, were obliged to submit a proposal for registration of data on beneficial owners with the respective register (the Commercial Register, Register of Non-Investment Funds, Register of Non-Profit Organisations Providing Welfare Services, Register of Foundations) no later than by 31 December 2019.

The legal persons registered in the Commercial Register, non-investment funds, non-profit organisations providing welfare services and foundations, which were established after 31 October 2018, are obliged to provide data on beneficial owners upon their establishment. The publicly available data on beneficial owners registered with the central Register of Legal Persons, Entrepreneurs and Public Authorities from 1 November 2020 include name, surname, date of birth, nationality, place of residence and data establishing the position of beneficial owner.

On 1 January 2021, based on Act No. 346/2018 Coll. on the Register of Non-Governmental Non-Profit Organisations and on the amendment to certain acts, the Register of Non-Governmental Non-Profit Organisations replacing the Register of Foundations, Register of Non-Profit Organisations Providing Welfare Services, and Register of Non-Investment

Funds was established. The Register of Non-Governmental Non-Profit Organisations is managed and operated by the MI SR.

Information on beneficial owners is also included in the Register of Public Sector Partners which was established based on Act No. 315/2016 Coll. on the Register of Public Sector Partners and on the amendment to certain acts as amended. The purpose of this act was to improve the transparency of entities in transactions with the State; the act contains a mechanism of verification of information on beneficial owners. The Register of Public Sector Partners is managed by the Ministry of Justice of the SR. Without a registration with the Register of Public Sector Partners, it is not possible to apply for resources from the state budget or take part in public procurement.

Vulnerabilities:

A low efficiency of implementation of data on beneficial owners into source registers was found, which results in low volume of data on beneficial owners in the central register (Register of Legal Persons, Entrepreneurs and Public Authorities); no efficient mechanisms are in place for the verification of correctness and topicality of data on beneficial owners of legal persons when provided to respective registers, as well as no mechanisms are in place for the application of appropriate and dissuasive sanctions if violations are detected in connection with the provision of data on beneficial owners; it is necessary to carry out a legal analysis of possibilities for the operation of foreign legal groupings (trusts) without legal personality if they operate in the SR (trusts without legal personality cannot establish a Slovak legal person providing capital to it or enter an already established Slovak legal person), and a legal analysis of operation of SR citizens in the position of foreign trust administrators. Filling the Commercial Register (and subsequently, filling the central Register of Legal Persons, Entrepreneurs and Public Authorities) with data on beneficial owners is also affected by the provision of Article 2 (3) of Act No. 530/2003 Coll. on the Commercial Register and on the amendment to certain acts, according to which the persons registered with the Register of Public Sector Partners are not obliged to provide data on beneficial owners to the Commercial Register.

No legal regulation in the SR imposes the duty to provide the central register with information on beneficial owners in legal groupings (trusts) upon the administrator of a legal grouping (trust) if the administrator of a legal grouping (trust) is a citizen of the SR with a place of residence in the (the duty of the SR resulting from Article 31 of Directive (EU) 2018/843 of the European Parliament and of the Council). As the Slovak legal system allows operation of silent partners in Slovak legal persons, it is necessary to pay an increased attention to identification of silent partners who can be considered beneficial owners.

E. Quality of criminal prosecution of financial crime

The basic precondition for efficient criminal prosecution is the ability and integrity of law enforcement authorities to commence and conduct criminal prosecution of criminal offences of legalisation of proceeds of crime. However, this must be preceded by efficient detection of legalisation of proceeds of crime, identification of proceeds and their movement,

and activities of competent authorities in the area of operational search and criminal intelligence.

E1. Capacity and resources for criminal prosecution in the area of financial crime

From 2016 to 2019, significant capacities of the Prosecutor's Office of the SR were allocated to penalisation of money laundering and subsequent property seizure. This was caused by the measures issued by the General Prosecutor of the SR which imposed the duty on prosecutors to execute financial investigations in specified criminal cases and ensured systematic collection of information concerning ML. These measures were updated on a regular basis also in compliance with the NRA process and Moneyval evaluation processes. In 2016, an active process of giving rise to criminal liability of legal persons started at the level of the Prosecutor's Office of the SR, in particular for criminal offences of economic nature. For objective reasons, specialisations for ML penalisation were not created at the level of the Prosecutor's Office because giving rise to criminal liability is closely related in particular to the penalisation of a predicate criminal offence. Educational activity of prosecutors in the area of ML and property seizure was also intensified – meetings concerning financial investigation take place on an annual basis.

Prosecutors investigating criminal offences of legalisation of proceeds of crime and predicate criminal offences work at all levels of prosecutor's offices, including the SPO, and are also directed by measures of the General Prosecutor of the SR. At work, they also use a methodological aid for financial investigation, as well as results of the processed evaluation of penalisation of the criminal offence of legalisation of proceeds of crime in the conditions of the SR.

In addition to the educational activities focused on ML and property seizure it should be pointed out that since 2016, educational activities have also been provided in connection with giving rise to criminal liability of legal persons and seizure of virtual currency, in which financial resources coming from crime can be placed. A leaflet for law enforcement authorities was prepared at the level of the Prosecutor's Office in this area.

Regional Prosecutor's Offices draw attention to the need to execute proactive and parallel financial investigation, which is the only possibility of identification and subsequent seizure of illicit income coming for the criminal activity, in particular in connection with drug-related criminal offences, criminal offences of trafficking in human beings, tax criminal offences and fraudulent activities with sham existence of contractual relations of business companies. The most important thing within efficient seizure of legalised proceeds of crime includes the timely exchange of information among banks and early provision of information to the Financial Intelligence Unit of the PPF, which continue to signalise the need of procedure pursuant to Article 95 of the Code of Criminal Procedure to investigators as well as to prosecutors. In practice this means that without the above institutions, a prosecutor alone has no real possibility to improve the efficiency of seizure of proceeds of this type of criminal activity.

In criminal proceedings after a bill of indictment had been filed, it was identified that some courts conditioned the fulfilment of signs of the objective aspect of the merits of criminal

offence of legalisation of proceeds of crime by the previous conviction of the perpetrator for a predicate criminal offence. In one criminal case, such opinion of district courts has already been confirmed by a resolution of a Regional Court. The General Prosecutor' Office of the SR did not identify with the draft cassation appeal of the prosecutor in this criminal case and considered it to be obviously unsuccessful and inefficient.

Joint trainings based on model cases, extension of Article 58/3 of the Criminal Code to other criminal offences and seizure in parallel with the filing of a bill of indictment or arrest of the perpetrator, as well as establishment of special analytical units are proposed as functional measures to eliminate the deficiencies.

Vulnerabilities:

A failure to adopt an act on the execution of asset seizure decision and seized asset management and on the amendment to certain acts seems to be the main deficiency for more efficient seizure of property in the assessed period. Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts came into effect on 1 January 2021. This Act will create real preconditions for the seizure of property and proceeds coming from criminal activities in particular in the cases of abuse of sophisticated schemes of economic activities of legal persons.

Moreover, it is necessary to ensure that every Prosecutor's Office consistently carries out financial investigation according to internal directions of the Prosecutor's Office and, at the same time, it is necessary to insist on criminal prosecution of legal persons. Solely this procedure will create preconditions for the efficient implementation of the quoted act on the execution of asset seizure decision and seized asset management and on the amendment to certain acts, with the fulfilment of the intended objective.

E2. Integrity and independence of law enforcement authorities in the area of financial crime

The criminal activity of investigators of financial criminal activities is at a level showing no significant year-on-year changes. No negative influence on investigators in connection with ML investigation and property seizure was found. The area of seized asset management and insufficient seizure of assets remains problematic; however, this is not caused by influence of other persons on the investigator, the reason is the insufficient use of financial investigation and legislative limitations in the area of asset seizure.

Investigation takes place without interventions, political or social pressure, corruption, intimidation or abuse of position and asset seizure takes place without undesirable external interventions. Investigators are procedurally independent by law. Pursuant to the Code of Criminal Procedure, only prosecutors supervise the lawfulness in pre-trial proceedings and in the proceedings prior to the commencement of criminal prosecution.

Statistics on criminal activities of investigators in executing cases of ML/asset seizure in general do not show a high rate of criminal activity in connection with corrupt behaviour in the area of ML and asset seizure.

At the level of DH PF and RH PF, property is seized to a small extent; the property to be managed is almost never seized taking into account the absence of an office managing the seized property. Orders for property seizure are issued by prosecutors or judges for pre-trial proceedings; asset management, in particular as regards immovable property, is complicated with respect to time and expertise. No authority, whose competence would include comprehensive seized asset management, was definitely appointed in the territory of the Slovak Republic in the assessment period. The asset management, which cannot be provided by the Police Force, is carried out by legal persons or government authorities. Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts, based on which the Asset Management Office is established, came into effect on 1 January 2021; the Asset Management Office itself should be established as of 1 August 2021.

The criminal activity of prosecutors within financial criminal activity is at a level showing no significant year-on-year changes. No negative influence on prosecutors in connection with ML investigation and property seizure was detected in the assessment period.

The prosecutor's supervision is carried out without intervention, political or social pressure, corruption, intimidation or abuse of position; property seizure is also carried out without undesirable external interventions. Prosecutors act independently by operation of law, the superior prosecutor cannot issue a so-called negative instruction against their procedure. In general, statistics of criminal activities of prosecutors during cases of legalisation/seizure of property do not show a high rate of criminal activity in connection with corruption in the section of property legalisation and seizure.

Vulnerabilities:

The absence of or insufficient legal regulation for identification of the assets to be seized, procedural procedures in seizing it really, and in particular during management of seized property in criminal proceedings were serious deficiencies in property seizure during criminal proceedings. Both the seizure of real estate as well as of business interests and other participating interests in legal persons are regulated insufficiently. With respect to the character of the seized property, in particular real estate but also participating interests in legal persons, as well as issues of turning it into cash, there is a real need to also ensure its management through professionally qualified persons. The above topics are regulated by Act No. 312/2020 Coll. on the execution of asset seizure decision and seized asset management and on the amendment to certain acts which came into effect on 1 January 2021. Based on this act, the Asset Management Office will be established with effect from 1 August 2021, which will ensure seized assets management either independently or through another person.

E3. Efficiency of national cooperation

To combat crime, the National AML/CFT Expert Group was established (NES-LP). Members of this group participate, inter alia, in the legislative activities in connection with adopting legislation in this area. NES-LP carries out its activities within the Interdepartmental Expert Coordination Body for Combating Crime.

Based on requests for collaboration, national cooperation within PF units is at a desired level. There is room for improvement – to speed up the process of request handling; however, this is affected by the current work load of the requested unit.

Within the PF, various trainings and methodical jobs are organised on a regular basis for various police units, in which employees of other ministries and Prosecutor's Office representatives also take part, if necessary.

Regular meetings of investigators with intelligence services, public authorities in the area of taxes, fees and customs, and with prosecutors are not arranged, as a matter of fact, nothing from the above is executed. The police cooperate with the Financial Administration within the "Tax Cobra" Project only to a limited extent. Exchange of information among the above authorities takes place in particular cases in the form of dissemination of information on UTs (FIU SR) and in the form of requests (e.g., the Financial Administration, Interpol, Sirene, ...). Individual DHs PF and RHs PF have meetings with competent District Prosecutor's Offices and Regional Prosecutor's Offices where officers from individual units of DHs PF and RHs PF participate.

As regards the Prosecutor's Office, improvement of qualification and exchange of experience is provided at all levels by organising regular collaboration meetings with the adoption of current measures.

As a matter of fact, there is no legal framework at the interministerial level allowing joint investigation of competent investigation units, and no such investigations are carried out. Investigation can be carried out in collaboration with other units.

According to the Regulation of the MI SR, a specialised investigation team can be established in particular in the event of criminal activity committed by an organised group or in the event of establishing, masterminding and supporting a criminal group or establishing, masterminding and supporting a terrorist group, whose detection, finding perpetrators and investigation is extraordinarily demanding taking into account its scope and way of performance, requires considerable effort and cannot be carried out by common forms or means. The establishment of the team and end of its activity usually takes place based on an order of the President of the Police Force, which also specifies the method of control by the team leader.

F. Quality of judgements

In the monitored period (2016 – 2019), there was no essential change of the judicial system in the Slovak Republic regarding the system of courts of the Slovak Republic or the court map (number of courts and their districts). The CEPEJ Project "Efficiency and quality of the Slovak judicial system" was implemented.

A more significant amendment to status acts in the judicial system[58] was approved in May 2017 and concerned three basic topics – selection procedures for judges, assessment of judges, and issues of disciplinary responsibility of judges[59]. More detailed information is provided below in Parts F.1 and F.2.

The competence of courts in relation to money laundering was not changed: general courts remain competent and in more serious cases, the Special Criminal Court is competent (as provided in detail in the previous NRA).

F1. Capacity and resources for judicial proceedings

Strengthening the efficiency and quality of the judicial system – CEPEJ Project

With respect to long-term adverse statistics regarding the length of judicial proceedings, as well as the long-term low confidence of citizens and entrepreneurs in the independence of the judicial system in Slovakia[60], the Ministry of Justice of the SR in cooperation with the European Commission for the Efficiency of Justice (CEPEJ) – Council of Europe implemented a project in 2017 – 2019[61], whose objective was to support the effort to strengthen the efficiency and quality of the Slovak judicial system. The main task was to achieve an improvement of the situation regarding law-suit handling and to maintain the quality of court decisions.

The Project was implemented in Slovakia during the period, when the Ministry of Justice worked on reform changes concerning the judicial system. They included, for example, a new court map, an effort to simplify some court procedures, the introduction of an electronic court payment order, the use of information systems and analytical tools for the improvement of court management and improvement of efficiency of courts. In this context, the CEPEJ reports contain several recommendations which can help further improve the judicial system in Slovakia.

[58] Act No. 152/2017 Coll.
[59] Important judicial changes have been implemented since 2020; they will be assessed in the next NRA.

[60] In 2019, the SR was in the EU in second (public assessment) or third place from the end (assessment by entrepreneurs).
61 The objective of the project is to strengthen the efficiency and quality of the Slovak judicial system through the assessment at national level and at court level, and application of tools and methodology of CEPEJ. The Project is divided into three stages: /i/ the assessment of the judicial system as regards efficiency and quality, including the CEPEJ recommendations to improve these aspects, reduce backlog and inadequate delays; /ii/ the assessment and recommendations of CEPEJ with the further development of the Analytical Centre and more efficient use of IT systems. The Analytical Centre is to be a key institution for the assessment of the whole judicial system and preparation of future reforms, and /iii/application of CEPEJ instruments and methodology for the management of courts' working hours and judicial system quality at selected court. It will be a form of training programmes for courts implemented at six selected courts, which will enable the application of CEPEJ instruments and methodology for the management of courts' working hours and, if necessary, also for the quality of the judicial system.

This activity of CEPEJ resulted in two reports:

- The first report with the title **Report on the state of the judicial system**[62] introduces an in-depth of the Slovak judicial system and consists of six parts: 1. Judicial system and court organisation, 2. Budget of the judicial system, 3. Judges and judicial staff, 4. Court management. Efficiency of courts, 5. Quality of courts and Executive summary. The Report on the state of the judicial system was officially introduced on 27-28 February 2018 to court representatives, legal professionals and journalists.
- The second report **Evaluation of the current state of affairs of IT tools for the Slovak judicial system and advice on their development** analyses the digitalisation of the judicial system mentioning the problematic aspects and offering solutions. Moreover, the second report also discusses the Analytical Centre and contains recommendations, which should ensure its successful operation.

In the third phase, the conclusions and recommendations resulting from the first and second reports **were implemented** using the CEPEJ tools and methodology. Working groups were appointed to adapt the recommendations and solutions resulting from the report to Slovak conditions. The phase of implementation should have lasted until January 2019; subsequently, it was extended to the end of June 2019.

Main findings of CEPEJ:

- It is important that **judges are specialised** into one of the main agendas (civil law, commercial law, family law or criminal law).
- **The court map should be reassessed** to achieve a better efficiency.
- It is necessary **to solve the problem of old enforcement cases,** also through a political solution in the form of an "emergency act".
- Human resources and financial resources should be allocated based on transparent and predictable tools.
- An increase in the number of judges does not seem to be necessary – courts must **better use the existing resources.**
- To ensure that a judge's family holiday or assignment to a higher-degree court does not cause problems.
- It is crucial **to use IT tools** to simplify the work of courts.
- It is crucial to have **reliable data** which will enable the execution of **informed decisions.**
- Clear specification of tasks in court administration and management.
- It is important to pay attention to differences in the performance of individual courts.
- Time frameworks should be introduced **which will set a time-limit for decision-making in a case,** thus achieving better efficiency.

62 The whole text of the "Report on the state of the judicial system" can be found HERE: https://www.justice.gov.sk/Stranky/Ministerstvo/Sprava-k-stavu-justicie.aspx

- Judges should be **more active in managing the cases** and endeavour to conclude them quickly.
- The use of the "flying judge" concept.
- It is necessary to ensure the consistency of case law.
- **Judgements** should be written in plain language and **briefer and clearer**.
- A communication strategy for court should be set.
- The use of **questionnaires for satisfaction surveys** aimed at court employees and court users.

The Project results in the gradual implementation of recommendations with a subsequent overall reform of the judicial system. The final goal of the judicial system reform is to improve the credibility of the judicial system, its performance and quality, and also to provide judges and court staff with better conditions for work and decision-making.

Financial and human resources

"The quality of judicial decisions presupposes, as a prerequisite, the proper organisation and functioning of the judicial system as a whole. The approach to quality is not then at the level of the judicial decision itself, but well beforehand, in the way in which the judicial system and the courts are going to be organised and will work. The postulate is therefore that a judicial decision of quality can be made only when the judicial environment lends itself to it, that it allows the judge to be effective and to carry out its work correctly. It is in this sense that we can speak of the administration of justice and management of courts as prerequisites for the quality of court decisions; and the assumption is that a quality court management will allow the courts/judges to make decisions of quality."[63]

The capacity to detect, investigate and prosecute criminal offences of legalisation of proceeds of crime is hindered by lack of resources and specialised analytical expertise at the Special Prosecution Office as well as in the National Crime Agency, and also problems with obtaining evidence.

The CEPEJ Report on the state of the judicial system in Slovakia, which was also worked out on the basis of surveys and discussions with judges, did not include lack of financial or human resources among the basic challenges.

In relation to the financial resources of courts, the CEPEJ Report mentioned the need to distribute them uniformly among individual courts, the need of uniform criteria of allocation of finances, and also proposed greater involvement of judges into the preparation of the budget.

As regards human resources at courts in general (both in relation to the number of judges and to the number of court employees) it surprisingly stated that the number of judges was

[63] Quotation: Report on the state of the judicial system in Slovakia, CEPEJ

superior to the European median[64]. This, however, does not exclude the variety of situations at individual courts.

Thus, the main problem consists in court management (including the assessment of the issue of court map) and in the need to modernise them by using suitable IT systems. It is recommended that all decisions, such as allocation of human resources or other categories of resources, division of tasks and work organisation, and time management be made on an informed basis.

Therefore, one of the first measures led to the establishment of an Analytical Centre within the Ministry of Justice of the SR so that all subsequent reforms could be adopted on an informed basis and based on data (data collection). The Analytical Centre was established in 2017. After some, time, this step can be assessed very positively.

The strategic role of the Analytical Centre[65]

"The Analytical Centre is a quite new body in the Slovak judicial framework. However, it plays an important role when it comes to the strategic vision of the Ministry of Justice. There are four different pillars that support this vision: "Evaluation and Analysis", "Modelling and Forecasting", "Statistics and Reporting" and finally "Cooperation". The Analytical Centre was set forward quite challenging goals: supporting the Ministry of Justice when drafting reforms, monitoring current trends for the policy makers, legislation assessment, evaluation of the courts' performance on a regular basis, etc. The team is currently composed of a good mixture of different professionals such as lawyers, economists, statisticians, data analysts and mathematicians. Such a professional amalgam is expected to be highly beneficial to the achievement of the set goals.

In regard to management of courts, the team of the Analytical Centre is called to a double task: interpreting past data on the performance of courts and extrapolating on past data to make predictions for the future. In an initial phase the Centre was mainly engaged in assessing all the data and information at its disposal. Now, since the team is enhanced in number and quality, it is focused on the development of a sound and robust methodology for data collection and information exchange."

The Analytical Centre has recently developed the concept of a new piece of software (AZU), which is designed for managing the collection of statistical data more efficiently. The testing phase of AZU within the pilot courts is now complete and final deployment took place from 1 January 2018.

---

[64] CEPEJ Report, quotation: "It results from the statistical data provided by the MJ that in 2016 there were 1215 active judges, while in 2015 there were 1211 active judges. The CEPEJ report "European judicial systems - Efficiency and quality of justice" (CEPEJ STUDIES No. 23), published in October 2016, indicates that in 2014 the number of judges per inhabitants in the Slovak Republic was superior to the European median (that is, 24.4 judges per 100,000 inhabitants, comparing to the European median of 17.82 judges per 100,000 inhabitants). Thus, in general terms, it is difficult to conclude that Slovakia faces a problem of insufficiency of judges. The same may be said in regard to court staff."

[65] Quotation: CEPEJ Project, Report Dec. 2017: Evaluation of the current state of affairs of IT tools for the Slovak judicial system and advise on their development

It also provides interactive statistics on the state of the judicial system (HERE):
https://web.ac-mssr.sk/
https://web.ac-mssr.sk/dashboard/

For the purpose of more flexible occupation of vacant judge positions and reduction of the process in occupying them, an amendment to Act No. 385/2000 Coll. on judges (by Act No. 152/2017 Coll.) was adopted with the objective to conduct mass selection procedures. The amendment introduces mass selection procedures at district courts, which will take place on a regional principle for the number of vacant positions of judge within a region undetermined in advance, in all eight regions on the same day. This mass selection will result in a list of candidates for the position of judge, who will subsequently go through necessary reviews and preparatory education, and will be prepared to occupy the vacant positions of judges.

In the monitored period, one of the CEPEJ recommendations was specified by adopting an amendment to the Act on Courts,[66] which introduced the concept of a visiting judge into the legislation, with the objective to create conditions for solving the situations temporarily negatively affecting court operation by causing a temporary absence of the legitimate judge.

Quality of decisions

Among the recommendations, besides the improvement of court management, the need of specialisation of judges also resonated, which is applicable to both the civil and criminal area. However, it can be introduced only at bigger courts. The above-mentioned supports the justness of a discussion about a change of the court map[67].

A survey concerning the quality of court decisions in the form of questionnaire was also carried out within the CEPEJ Project. According to CEPEJ, the responses to the Quality Questionnaire did not show any particular problem in connection with the overall justice of proceedings at Slovak courts. Various actors speaking to CEPEJ (Slovak Bar Association, non-governmental organisations) did not signalise any particular problem concerning alleged injustice of judicial proceedings, either.

However, certain criticism can be noticed in relation to the clarity of judicial decisions. The report mentions: "As concerns the clarity of judicial decisions, reference has to be made to the well-established practice of Slovak judges, confirmed by the Questionnaire on Quality (87 % of positive answers), to offer quite a detailed reasoning in fact and law to their decisions. However, a few critical points emerge from the comments to the Questionnaire on Quality. Some of the respondents indicated that too much space of the decision is occupied by the

[66] Amendment - Act No. 282/2019 Coll.

[67] CEPEJ Report, quotation: "It emerged from the discussion with representatives of the MJ and of the judiciary, as well as from the comments to the replies to the Questionnaire on Quality, that judges are not satisfied with the present court organisation, in particular with the high number of district courts (which doubled between 1993 and 1998). Some are of the opinion that several district courts should be either closed down, or merged in one bigger district court as courthouses. Each courthouse should then deal with a given type of cases (labour cases, criminal cases, family law cases etc.), in order to pursue a higher specialisation. This issue has to be addressed in connection with the analysis of the Slovak judicial map."

description of proceedings, quoting from the minutes of the hearings, without any synthesis of the factual elements which are truly relevant for the legal reasoning. Some other respondents casted doubts over the relevance of the legal arguments written in the rather extended text of judicial decisions, as sometimes they do not provide a clear explanation for the case under examination, but often veer off to various formal elements."

Within the conclusions, however, it states: "It cannot be excluded that the widespread practice of providing a detailed reasoning in fact and law in judicial decisions of Slovak courts reveals a rather formalistic approach. On the contrary, it has to be recalled that an effectively reasoned decision shows to the parties that their case has truly been heard and contribute to the trust of the public in the judiciary in a democratic society. A highly detailed and complex motivation risk to undermine the comprehensibility of the decision and to have a negative effect on the efficiency of justice. Therefore, the need for a detailed reasoning has to be adapted to the nature of the decision and to the circumstances of the case. Parties are generally entitled to a reasoned answer to their main legal arguments and pleas."

Taking into account the above-mentioned, it cannot be concluded that the quality of judicial decisions is low. It appears to be adequate. However, it is necessary to further discuss the quality of judicial decisions including in the area of money laundering. In some aspects, the LEAs indicated dissatisfaction with the absence of resolution of some issues in judicial decisions or mentioned the disunity of case law (which was also another challenge for improvement in the Slovak judicial system according to the general CEPEJ assessment).

Current need of specialisation

Although it can be assumed that judges with greater or smaller experience in money laundering cases work at general courts, it should be noted that there is no systematic specialisation of judges of general courts in this area. Such specialisation can be observed at the Special Criminal Court.

This statement is also supported by the conclusions of the CEPEJ Report:

"It has been particularly highlighted by all the national stakeholders participating to this evaluation exercise that one of the most important issues for the Slovak judicial system is that of specialisation of judges. According to representatives of the MJ, the prevailing consideration is to reach, at the same time, quality and efficiency. Several judges, in the process of developing the present report, underlined their approval to the possibility to increase their specialisation in specific areas of law, going even further the very general distinction between civil and criminal cases. In their view, each judge should ideally be in charge of just one type of agenda, which is admittedly difficult to achieve at the level of small district courts and at the level of regional courts. Representatives of the Bar Association support the specialisation of judges. On the contrary, the "causal jurisdiction" does not seem to be considered as the best tool to achieve judges' specialisation.

In this regard it can be added that 54% of the replies to the Questionnaire on Quality were negative as concerns the need to create or to maintain the existence of specialised courts in the Slovak judicial system, while only 25% were positive. Moreover, although not favourable

to the specialisation of courts, the respondents supported the specialisation of judges. Thus 64% of all respondents (and 71% among the respondents who are judges) replied "Yes" to judges' specialisation, 13% (10% among the respondents who are judges) said that it is partially necessary and 23% (19% among the respondents who are judges) replied "No."

Quality of cases – change of trend

As regards the quality of cases, as it has been mentioned above, despite an increase in cases/criminal proceedings concerning the criminal offence of legalisation of proceeds of crime, mostly less serious criminal offences were concerned. For the period 2016 – 2019, however, a positive change of the trend can be mentioned thanks to all judicial power units. In this context, only the year 2020 seems to mean a turning point, however, it is not included in this National Risk Assessment.

Statistics

Detailed statistics of the numbers of commenced criminal prosecutions, numbers of persons indicted persons and subsequently convicted of the criminal offence of legalisation of proceeds of crime are provided in the THREATS part.

Articles 233/234	2016	2017	2018	2019
Commenced criminal prosecutions	130	209	149	66
Indicted persons	39	58	20	32
Convicted persons	17	26	18	13
Asset-related decisions (Articles 58, 60, 83 of the Criminal Code)	4	6	1	5

Education of judges

Education of judges (and prosecutors) is provided in particular by the Judicial Academy in the form of preparatory education (pre-examination preparation) and lifelong education in compliance with the following conceptual documents:

a) The contents of education of judges for 2016 – 2020[68],
b) Concept of education of the Judicial Academy (from 2016, updated in 2019), worked out in compliance with the recommendations and resolutions of the European Parliament and of the Council of the European Union[69];

[68] The contents of education of judges is specified (based on an agreement with the Minister of Justice) and approved by the Judicial Council of the SR
[69] Recommendation No. 2006/962/EC, Resolution No. 11114/08, Commission Communication No. 14196/11)

c) The contents of education of judges and preparatory education of candidates for the position of judge approved by the Judicial Council of the SR in 2017.

The full texts of reference documents are available at the website of the Judicial Academy HERE:

https://ja-sr.sk/obsahova-napln-sudnej-rady-sr-generalneho-prokuratora-sr-koncepcia-vzdelavania-rady-justicnej

Preparatory education

Pre-examination education takes place before a professional judicial examination is taken. To a certain extent, the preparation for examinations can be considered part of preparation for further career growth. After the successful mass selection procedure or selection procedure for a higher court, within educational events, the Judicial Academy organises preparatory education of candidates for the position of judge. The completion of preparatory education is a necessary precondition for further progress before the appointment to a position of judge.

Education of a particular group of judges takes place in the period of three years according to specialisation and assignment at the respective court. Professional preparation is organised in the form of professional lectures and workshops (6 – 8 workshops lasting two days each in the course of three years) (cyclic education in linked blocks).

Lifelong education

Lifelong education as well as language education is provided by the Judicial Academy for the whole target group, i.e., judge, prosecutor, senior court officials, court trainees, assistants to judges of the Supreme Court of the SR, Prosecutor's Office legal trainees, secondary education of probation and mediation officers and court secretaries.

For the reason of methodology and continuity of educational process, lifelong education is divided into two parts within the definition of the target subgroup:

- junior judge with the length of professional experience from 0 to 4 years,
- senior judge with the length of professional experience of four and more years.

The objective of lifelong education for junior judges is to familiarise them with the development of theory and practice of the judiciary in the Slovak Republic, subsequently, with the practice in a broader European context, and to provide them with knowledge, skills and work habits needed for the position. Special attention should be paid to specialisation in individual legal areas (civil, criminal, commercial and administrative law).

The objective of the 2nd degree of lifelong education for senior judges is to focus on the agenda of judges of regional and district courts, as well as on the decision-making activities of the Supreme Court of the SR (the emphasis will be on positive legal regulations based on the specialisation of judges on the basis of suggestions from relevant entities) and new legal standards. Another part of education will be focused on cultivating the personality of a judge

and their soft skills. This would include in particular lectures on psychology, speech and especially ethics.

Number of educational activities and their topics

The number of educational activities of the Judicial Academy depends on the number of business days in the year and on spatial and personnel capacities. The topics of educational events are determined in accordance with the contents submitted by the GPO SR and the Judicial Council of the SR. In general, education is provided to the whole primary target group.

Summary of activities of the Judicial Academy (Annual Reports) is available at its website HERE: https://ja-sr.sk/vyrocne-spravy-justicnej-akademie-slovenskej-republiky

Educational events of the Judicial Academy in figures

Year	Number of educational events	Number of participants
2016	141	4849
2017	96	3916
2018	26	5343
2019	131	5275

The summary of event topics can be found at the website of the Judicial Academy HERE:
https://ja-sr.sk/archiv-studijnych-planov-kalendar-vzdelavacich-podujati .

As regards the education in the area of money laundering in 2016-2020, educational events generally or partially focused on this area were carried out every year:

Year	Number of education days	Topic
2016	2	Fight against corruption including OECD and GRECO Group recommendations
	2	Tax delinquencies and application practice of courts of the SR and of the Financial Directorate of the SR
	2	Seizures and confiscations (Brussels)
	1	Seizure of property in criminal proceedings (a national event)
	4	New paths for a better cooperation between judiciary and police in the field of fight against drug trafficking (Antwerp)
	2	Judicial cooperation in criminal cases of the EU. Prejudicial issues in criminal cases (Sofia)
	2	International judicial cooperation in criminal cases (Bucharest)
	4	Financial investigations and asset recovery for THB investigations (Vienna)
	2	Legal contact with foreign countries

2017	1	Corruption in the public sector
	1	Organised crime and transnational organised crime
	1	Current decision-making practice in relation to property seizure in criminal proceedings
	2	Tax system and tax proceedings, application practice of courts of the SR and the Financial Directorate of the SR (Omšenie)
	4	Cross-border cooperation – financial investigation
	1	Persons entitled to act for business companies – position and responsibility (a national event in Pezinok)
	2	Criminal liability of legal persons (Omšenie)
	2	Legal contact with foreign countries (Omšenie)
2018	1	Activity of criminal groups and migration
	2	Financial investigation
	2	Corruption in the public sector
	2	Latvia, Riga – Protection of financial interests of the EU
	2	Legal contact with foreign countries in criminal cases (Field Office of the Judicial Academy of the SR Omšenie), Operational Programme Effective Public Administration
	5	The Netherlands – Financial investigation and property confiscation
	2	Spain, Madrid – Property confiscation in the EU
2019	2	European Public Prosecutor's Office
	2	Application practice in the cases of criminal liability of legal persons (CR – comparative perspective), Field Office of the Judicial Academy Omšenie, Operational Programme Effective Public Administration
	5	The Netherlands, Apeldoorn- Fight against terrorism and terrorist financing
	2	Criminal offences related to debtor's bankruptcy and tax optimisation (Field Office of the Judicial Academy Omšenie) Operational Programme Effective Public Administration
	2	Greece, Thessaloniki – Protection of financial interests of the EU and EPPO
	1	Tax delinquencies and application practice of courts of the SR and of the Financial Directorate of the SR (a national event of the Judicial Academy of the SR Pezinok)
	2	Croatia, Zagreb – Criminal offences of economic nature: Property confiscation and confiscation in the EU

As regards education in the area of judicial ethics, it was included in the preparatory education in the monitored period. As part of lifelong education, the number of activities ranged from 2 to 4 annually. Similar knowledge can be deduced in relation to soft skills.

Vulnerabilities:

Pursuant to Article 30 (7) of Act No. 385/2000 Coll. on judges as amended, judges are obliged to improve their expertise and use the offered possibilities of education. However, the participation in particular educational activities, either organised by the Judicial Academy or by other entities, is voluntary. In this context support measures leading to a mandatory time framework for completing selected educational activities can be considered with the objective to ensure progressive and continuous education with the support of specialisation. The CEPEJ Report recommends mandatory initiatory education of judges.

Despite the great quantity of events more or less concerning money laundering, no activity exclusively focused on this criminal activity was identified in the monitored period. In this context, it would be suitable to consider systematic specialised and even interprofessional and interdisciplinary education with the objective of specialisation of judges.

A special question is the question of strengthening/intensification of education in the area of judicial ethics and integrity in general.

However, for the objectivity of assessment it should also be noted that the Judicial Academy is only one of several entities providing education. Judges also learn by self-studying or take part in other activities within their courts or participate in events organised out of the judicial sector through other entities (faculties of law, private sector in the area of legal educational activities).

F2. Integrity and independence of judges

As regards the legislative conditions of independence of judges, there were no essential changes in the monitored period, although partial changes were made concerning disciplinary proceedings, temporary suspension of performance of the function of judge and introduction of public hearing of constitutional judges.

The fact that the basis of guarantees of judicial independence is included in the Constitution of the SR is still valid. The independence of the judicial system from the other State power components results from Article 141 of the Constitution, according to which the judiciary in the Slovak Republic is performed by independent and impartial courts. The judiciary is performed at all degrees separately from other State authorities. Judges are appointed and removed by the President of the Slovak Republic on the proposal from the Judicial Council of the Slovak Republic. In performing their function, judges are independent and in decision-making they are bound by the Constitution, constitutional acts and relevant international treaties. A temporary suspension of performance of the function of judge must not interfere with independent performance of the judiciary. The reasons for interruption of performance of the function of judge, as well as conditions for the temporary suspension of performance of the function of judge or for temporary assignment of a judge are laid down by law. Judges must not be prosecuted for decision-making including after the end of their functions. A judge may file a complaint against a decision on the commencement of criminal prosecution of judge; the decision on the complaint shall be made by the General Prosecutor.

The judicial system of the Slovak Republic consists of district courts (54), regional courts (8) and the Supreme Court of the Slovak Republic. The judicial system also includes the Special Criminal Court.

The Special Criminal Court is a court of first instance with a national competence for the most serious criminal offences concerning the organised crime, criminal offences against property and criminal offences of economic nature, as well as corruption-related criminal offences and the most serious criminal offences committed by public figures in connection with performance of their functions. In 2017, its competence was expanded with extremism-related criminal offences.

In January 2019, the Constitutional Court decided that reviews of judges based on information from the National Security Authority, which raised serious concerns over the independence of the judiciary, were unconstitutional.

Measures to strengthen the credibility of the judicial system

As regards the perceived independence of the judiciary, the Slovak Republic is among the last EU Member States.

Confidence of citizens and entrepreneurs in judicial independence in the SR has been a long-term problem. After the murder of Ján Kuciak and his fiancée in spring 2018, and subsequently, after the communication of indicted M.K. with several judges, prosecutors, politicians and other people via the Threema application had been publicised in media, confidence in state institutions and especially in the judiciary even decreased.

The information publicised in media led to a temporary suspension of some judges and prosecutors. Although the above-mentioned confirmed the existence of securing mechanisms for such situations, a pressure on the improvement of their efficiency came into existence. Discussion on the real efficiency of disciplinary proceedings for judges and on the needed changes, which would return confidence in justice, was started.

Most causes at the end of the monitored period were cases of corruption.

As an immediate response, an amendment to the Act on Courts and Judges[70] was adopted, implementing a set of measures, which should *temporarily* prevent *active* performance of function of judge for those judges, for whom there are *reasonable doubts* as to the fulfilment of conditions of competence if it can seriously endanger the credibility or reputation of the judicial system. The decision on a temporary suspension of the performance of function of judge is made by the Judicial Council on the proposal from the President of the Judicial Council, Minister of Justice or President of the Supreme Court. The active performance of function of judge can be temporarily suspended for maximum six months, with the possibility of extension by additional six months; however, it must not exceed a total length of 12 months.

70 Amendment – Act No. 459/2019 Coll. (Article 22a) of 5 December 2019

With respect to the planned replacement of judges of the Constitutional Court of the SR in 2019, the MJ SR also prepared new rules for appointment of constitutional judges from 2018. Eventually, a general political agreement on a change of the Constitution was not reached; however, an agreement on the introduction of public hearing of candidates for constitutional judges within a new Act on the Constitutional Court (Act No. 314/2018 Coll.) was reached. This was implemented with a positive public reaction. Such practice can be considered a good measure for strengthening the confidence in the judicial system.

A new Act on the Constitutional Court of the Slovak Republic from October 2018, which replaced Act No. 38/1993 Coll. on the organisation of the Constitutional Court of the SR, on proceedings before it and on the position of judges, was adopted with the objective to strengthen the protection of fundamental rights by improving the efficiency of work of the Constitutional Court, reacting to its current experience.

Amendment to Act No. 385/2000 Coll. on judges from 2017:[71] as regards the changes in the assessment of judges, it will be carried out by professional assessment commissions at district and regional courts. Only a judge or a judge emeritus can be elected as a member of an assessment commission. A separate assessment commission should be appointed within each region; a commission will assess judges from another region. Members of an assessment commission are elected and removed by the Judicial Council. The judge elected as a member of an assessment commission does not perform the function of judge; membership in an assessment commission is considered performance of function of judge. The assessment of a judge shall be published at the website of the ministry. Repeated negative assessment of a judge remains a serious disciplinary misconduct and three consecutive negative assessments of a judge result in disciplinary liability with the possibility of termination of the function.

As regards disciplinary liability of judges, the objective of the change[72] was to improve the efficiency of disciplinary proceedings. The amendment also establishes the authority responsible for the oversight of smoothness of disciplinary proceedings - the Judicial Council of the Slovak Republic[73].

Fulfilment of international recommendations

The Group of States against Corruption (GRECO, Council of Europe)**[74]**

The Slovak Republic was assessed in the 4th round of GRECO evaluation in October 2013. GRECO addressed several recommendations concerning the judicial system to Slovakia, in particular as regards the adoption of Codes of Ethics, a modification of composition of the Judicial Council, changes in the legal regulation of removal of court presidents, extension of

[71] Amendment - Act No. 152/2017 Coll.
[72] Amendment - Act No. 152/2017 Coll.
[73] After the establishment of the Supreme Administrative Court, the questions of disciplinary proceedings for judges will be assessed by this court.
[74] The evaluation of the Slovak Republic was completed in 2020 with a relatively bad result due to the absence of fulfilment of recommendations concerning Members of Parliament.

the scope of information published in asset declarations (in particular as regards received gifts), adoption of a comprehensive strategy for the prevention of any conflict of interests for judges.

The following GRECO recommendations in relation to the judicial system were completely fulfilled in the monitored period:

- *recommendation vi* = that decisions to remove court presidents be reasoned, and are made subject to judicial review (removal) – completely fulfilled in 2017
- *recommendation ix* = that a focused policy for preventing and managing conflicts of interest and corruption risks within the judiciary be elaborated and properly enforced – completely fulfilled in 2017
- *recommendation xi* = ensuring a more in-depth scrutiny of the declarations – completely fulfilled in 2019 by cancelling the limit of EUR 50,000 for the assessments of increase in assets and strengthening human resources for the control of asset declarations.

The following recommendations remain partially fulfilled:

- *recommendation viii* = the "Principles of Judicial Ethics" should be revised and further developed (GRECO considers the Code of Ethics to be only generally formulated) – there are no interpretation rules for the Code of Ethics
- recommendation x = establishing an obligation to declare liabilities (e.g. debts and loans) and gifts above a certain value on judges
    - As a follow-up to the requirement of GRECO, the amendment to the Act on Courts and Judges from 2017 laid down the judges' duty to declare contractual relations in asset declarations (including gifts) exceeding €6,600 (note: an identical duty was laid down for prosecutors). However, despite the above-mentioned, GRECO expressed doubts about the adequacy of the limit of €6,600 with respect to judges' salaries and to the average income in the national economy. The SR reassesses the possibilities of fulfilment of the above recommendation.

Statistics

Court presidents as representatives of the judicial system are authorised by the Ministry of Justice of the SR to hold judges accountable for disciplinary misconduct (also see Article 42 (3) of Act No. 757/2004 Coll. on courts). It is because court presidents should know the circumstances of the case, the judge's work load or their personal conditions. Before a proposal for disciplinary proceedings is filed by the Minister of Justice, the ministry asks the competent court president to provide an opinion on the possibility of disciplinary prosecution of the judge. If the court president does not file the proposal and the failure still appears to be a disciplinary misconduct, the minister shall file a proposal for disciplinary proceedings.

Year	Number of motions for disciplinary proceedings concerning judges	Of which: lodged by the Minister of Justice
2016	29	7

2017	30	5
2018	14	6
2019	13	3

Records of disciplinary proceedings are kept by the Office of the Judicial Council.

Vulnerabilities:

The crisis of the judicial system seen at the end of the monitored period can also be perceived as a crisis of integrity. The absence of a Code of Conduct, which would supplement the general provisions of the Code of Ethics with sample life situations and other practical examples, appeared to be a serious problem.

Greater attention should also be paid to the area of ethics within the preparatory and lifelong education of judges.

It will be necessary to ensure the consistency of case law and the uniformity of court procedures more thoroughly, as well as to better communicate the court decisions to the public.

Strengthening the transparency, for example, by introducing public hearings for important judicial posts, appears to be a suitable practice for society as a whole in order to improve the confidence in the judicial system.

G. Quality of framework for property seizure and withdrawal of proceeds of crime

Quality of framework for property seizure depends on the following factors (except for the factor "comprehensiveness of acts on property seizures", the other factors were evaluated in the previous articles):

- quality of collection and processing of intelligence information by the FIU SR,
- capacities and resources for the investigation of financial criminal activity, integrity of investigators of financial criminal activity,
- capacities and resources for criminal prosecution in the area of financial criminal activity,
- integrity and independence of criminal prosecution in the area of financial criminal activity,
- capacities and resources for judicial proceedings,
- integrity and independence of judges,
- comprehensiveness of acts on property seizures,
- availability of reliable information and evidence,
- efficiency of national cooperation,
- efficiency of international cooperation.

Legislation allows seizing the income and means coming from ML and its predicate criminal offences, profits derived from these criminal offences and the property of respective value owned by the accused person.

A protective measure of confiscation of a thing which, as a sanction, can also affect property of a person other than the perpetrator, can be imposed. Inter alia, a thing of a third person can be seized for the purposes of confiscation of a thing (Article 461 of the Code of Criminal Procedure), as it is possible to impose a protective measure of confiscation of a thing which, as a sanction, can also affect property of a person other than the perpetrator

.

Property can be tracked pursuant to Article 3 of the Code of Criminal Procedure, according to which a policeman can ask state authorities, higher territorial units, municipalities and other legal persons and natural persons for information on property and income of persons. Operational-search activities and intelligence activities (in particular FIU SR) can also be used to find property and income. Property is also searched for by screening records available to PF members (MI, informative abstract of the Real Estate Register).

Essentially, the SR has the necessary legal possibilities although with some deficiencies. In some cases, seizure is only possible from an accused person, i.e. only after a charge has been brought. Only an accused person's property can be seized as a whole.

The Code of Criminal Procedure provides a wide scale of tools for property seizure but application problems are connected with some seizure instruments.

In the monitored period, there were only several legislative changes leading to the strengthening of some concepts of criminal law, by amending the Code of Criminal Procedure by Act No**. 397/2015** Coll. with effect from 1 January 2016:

- seizure of a thing for the purpose of enforcement of the penalty of forfeiture of a thing and protective measure of confiscation of a thing was enabled (see the change in Article 428 (2) and a new section (2) in Article 461 of the Criminal Code),
- it was enabled to confiscate a thing which does not belong to the perpetrator and was obtained through a criminal offence or as a reward for a criminal offence or it was obtained for such things (see the supplementation of Article 83 (1) with new letters (c) and (d) of the Criminal Code).
-

The evaluation of the Moneyval Committee from the 5th round of evaluation critically mentioned several application and legal deficiencies connected with the quality of framework for property seizure and withdrawal of proceeds; it is possible to agree with main aspects of them.

Insufficient financial investigation is the first basic deficiency.

In this connection, there is a permanent problem of (non-)determining the value of the property where there is no agreement on the authority that should provide it (investigator, prosecutor or court).

Another essential deficiency is a relatively low efficiency of seizure of a thing/property in complex cases of money laundering. A negative impact of the non-existence of an Asset Management Office was clearly seen in complex cases. The absence of detailed rules and procedures in managing the seized property in pre-trial proceedings was another identically serious deficiency. Very simply it can be stated that the legal framework valid in the monitored period is efficient in seizing movable things, simple objects. If real estate, a real estate complex or an enterprise is concerned, the system fails. Exactly this aspect – the problem, *what (to do) with seized property* – often led to the decision to not seize the property. The Moneyval's requirement leads to the ability to ensure *active* management of seized property (not only its safekeeping). Key recommendations of Moneyval are in this context justified[75].

The deficiencies of legal regulation were also seen in the possibility of property transfer to third/close persons without an efficient possibility of making an objection to the validity of such acts. This deficiency was seen both in the pre-trial phase or in the phase of judicial proceedings, and in the phase of exercise of property-related decisions (especially the penalty of forfeiture of property[76]).

The Moneyval finding mentions in this context: "The legislation does not expressly cover the confiscation of laundered property. ... Confiscation of laundered property does not seem to be expressly covered by law and the coverage of third-party confiscation is still incomplete. Simply said, it is a problem of "transferring" laundered assets to third persons."

The third finding of the assessment process is the inability of the Slovak Republic to prove the efficiency at a stage of exercise of property-related decisions, in particular in the event of exercise of the penalty of forfeiture of a thing (in particular immovable thing) and forfeiture of property. There is no systematic data collection. The data is not kept systematically by competent authorities – district offices because they have never been requested to do so. No separate accounting records of confiscated property within criminal prosecution are kept, thus, there is no data on the really withdrawn proceeds of crime.

The conclusions of the first National Risk Assessment concerning the need to establish a Central Register of Bank Accounts or the need to improve efficiency of the Act on Proving the Origin of Property remain valid.

Besides the above knowledge it should be added that the Moneyval evaluation drew attention to the protection of rights of third persons in using the provisions of Article 83 (1) (c) and (d) of the Criminal Code.

Protection of third parties' rights acquired in good faith is solved through case law in compliance with Decision of the Constitutional Court of the SR I. ÚS 549/2015-33. The problem is monitored by Moneyval and although its requirement is directed to the regulation of the problem by material-law regulations (positive law), the argumentation

[75] Moneyval evaluation: "The authorities should urgently review the legal and procedural framework for forfeiture/confiscation to identify the possible issues in the process and take appropriate steps to ensure that criminal proceeds are effectively confiscated in all cases. (IO8)."
[76] See, for example, the Baštrnák example and other.

of the Slovak Republic was accepted in the process of evaluation. However, in the future practice it will be necessary that the rights in property of the acquirer in good faith received constitutional protection in compliance with the above-quoted decision of the Constitutional Court from 2016.

Confiscations without previous conviction were not introduced into law of the Slovak Republic.

In November 2018, a regulation on the mutual recognition of freezing orders and confiscation orders was adopted, however, its real application started only in December 2020.

As regards international cooperation, no significant deficiencies with an important impact on practice were recorded in the monitored period; this was also confirmed by the Moneyval Report.

Statistics:

Asset-related decisions Basic overview Number									
		Number							
			2013	2014	2015	2016	2017	2018	2019
The penalty of forfeiture of property	Article 58 of the Criminal Code	ML	0	0	1	2	2	2	1
		other	9	4	24	15	23	23	48
The penalty of forfeiture of a thing	Article 60 of the Criminal Code	ML	0	0	0	1	1	2	1
		other	975	968	870	821	855	863	1400
Protective measure Confiscation of a thing	Article 83 of the Criminal Code	ML	0	0	0	0	0	1	-
		other	84	54	94	51	63	71	-

Vulnerabilities:

It is necessary to establish and put into operation the Asset Management Office in order to ensure active asset management including more complex cases.

It is suitable to strengthen and expand seizure concepts, including the possibility of seizure of another property or substitute value or participating interest in a legal person.

The shortcoming is that information obtained by PF units according to a legal regulation other than the Code of Criminal Procedure, must be requested again by the investigator pursuant to the Code of Criminal Procedure.

A missing central register of bank accounts and the impossibility to monitor bank accounts online represents an essential problem. There is no possibility at all to monitor property, the state can be assessed only by repeated sending of requests to competent institutions; this is not active monitoring of property in real time.

It will be necessary to create a system of data collection with the objective to ensure the possibility of regular evaluation of efficiency of not only the system of seizure of things and property and its management, but also of the real withdrawal of proceeds of crime.

Vulnerabilities:

Property of third parties cannot be seized except for the perpetrator's property mixed with property of a third party. A substitute value cannot be seized from third parties, either. The shortcoming is that information obtained by PF units according to a legal regulation other than the Code of Criminal Procedure, must be requested again by the investigator pursuant to the Code of Criminal Procedure.

A missing central register of bank accounts and the impossibility to monitor bank accounts online represents an essential problem. There is no possibility at all to monitor property, the state can be assessed only by repeated sending of requests to competent institutions; this is not active monitoring of property in real time.

However, the current legislation does not allow seizing things and property to a sufficient extent because is some cases seizure is possible only for an accused person (i.e. after a charge has been brought, which can take some time); therefore, the current legislation concerning the seizure of a thing and property cannot be considered legislation allowing in all cases a prompt procedure and fast seizure.

In relation to seizure of assets and management of seized assets, in 2020, the act on the execution of asset seizure decision and seized asset management and on the amendment to certain acts was approved, which, inter alia, establishes a separate Asset Management Office. Within the new legal regulation, new merits of the criminal offence of legalisation of proceeds of crime will also be defined including a new structure of provisions concerning the seizure of things. A limited ability of authorities to detect, seize and withdraw illicit property within the fight against crime remains a vulnerability of the country.

Sources of information: IMF, www.openiazoch.sk, doc. Ing. Ladislav Kareš, PhD., University of Economics in Bratislava, Faculty of Economic Informatics, Department of Accounting and Auditing, Report: Efficiency and quality of the Slovak judicial system, assessment and recommendations on the basis of tools of the European Commission for the Efficiency of Justice (CEPEJ).

6. RISK ASSESSMENT IN CONNECTION WITH VIRTUAL CURRENCIES

Virtual currencies (e.g., Bitcoin, Litecoin, Ethereum and other) are not recognised in the Slovak Republic as official national or foreign currencies, do not represent electronic money in accordance with the act on payment services, and do not have any physical counter-value in the form of a legal means of payment. Despite that, in this area a permanent dynamic development can also be seen in our country, both in terms of technology and in terms of an increasing number of entities operating on the market of virtual currencies and services, whose offer directly correlates with the adequately increasing demand for virtual currencies in the population. No special requirements are in place for such trade (e.g., a licence issued by the National Bank of Slovakia), and for business activities only a general free trade licence was sufficient until recently and these entities were not subject to AML supervision/control until recently.

The continuous and fast technological development on the one hand in connection with the length of legislative processes at both European and national levels on the other hand represent the biggest limits in setting an optimum legal framework of regulation and control in this area.

The bases of the legal framework for virtual currencies have been gradually included in Slovak law since 2018.

On 1 October 2018, Act No. 213/2018 Coll. on insurance tax, and Act No. 431/2002 Coll. on accounting to an extent of definition of terms concerning virtual currencies and their taxation came into effect.

The above amendments were preceded by Methodical Guide of the Ministry of Finance of the Slovak Republic No. MF/10386/2018-721 on the procedure of taxation of virtual currencies (hereinafter the "Methodical Guide"), which ensures the uniform interpretation in imposing taxes on income flowing from the sale of virtual currencies pursuant to Act No. 595/2003 Coll. on income tax as amended, amending certain acts. According to this Methodical Guide, the income from the sale of virtual currency is also considered taxable income according to the Act on Income Tax.

The sale of virtual currency, including the exchange of virtual currency for property, exchange of virtual currency for another virtual currency, exchange of virtual currency for the provision of service or transfer of virtual currency for consideration, is considered taxable income.

The Methodical Guide also specified the definition of virtual currency, which means a digital carrier of value, which is not issued or guaranteed by a central bank or public authority, and is not necessarily bound to a legal means of payment, does not have a legal status of

currency or money but it is accepted by some natural or legal persons as a means of payment and which can be transferred, stored or traded electronically.

On 1 November 2020, an amendment to the AML Act came into effect and assigned the entities providing services connected with virtual currencies to the obliged entities: they included the providers of services of cryptocurrency wallet and providers of services of virtual currency exchanger, who provide professional services of exchange between virtual currencies and fiat currencies (i.e., coins and banknotes designated as legal means of payment and electronic money of the country received as the means of exchange in the issuing country).

At the same time, the amendment to the AML Act also amended, with effect from 1 November 2020, Act No. 455/1991 Coll. on trade licencing, based on which the providers of services of virtual currency exchanger and the providers of services of cryptocurrency wallet were included among regulated trades.

The assignment of the providers of services of cryptocurrency wallet and providers of services of virtual currency exchanger to obliged entities is based on the provisions of the 5th AML Directive.

The AML regulation of these entities was caused by the fact that the providers of services of virtual currency exchanger exchanging virtual currencies for uncovered fiat currencies, as well as the providers of services of cryptocurrency wallet were not subject to any legal duty to identify suspicious activities. A combination of the absent regulation in connection with natural features of virtual currencies, such as a higher rate of anonymity, complicated tracking of transactions or the possibility to use technological means to conceal the origin caused that for terrorist groups or perpetrators of criminal activities, virtual currencies became a simple tool for the transfer of financial resources to the financial system of the EU or to conceal their origin in a criminal offence.

However, already the 5th AML Directive has stated that by including the providers of services of virtual currency exchanger exchanging virtual currencies for fiat currencies and the providers of services of cryptocurrency wallet among obliged entities, the problem of anonymity connected with transactions of virtual currencies carried out by terrorist or criminal structures for the commission of criminal activities or money laundering will not be fully solved because a great part of the environment of virtual currencies will further remain anonymous and unregulated.

Therefore, including in connection with the prepared comprehensive regulation of the sector of virtual assets within the European Union,[77] in future, the area of obliged entities will have to be specified in an extensive manner and all providers of services of virtual assets also covering potential virtual currency exchanges, investment advisors or operators of virtual currency ATMs, will have to be included among obliged entities.

Today, the issue of integrity is examined only in relation to the trade operator. As a follow-up to FATF recommendations No. 15, the Slovak Republic should also adopt legal or regulatory measures which would also assess this fact in relation to holders or beneficial owners of a significant interest of the provider of services of virtual assets.

It will also be necessary to set a system of measures focused on the identification of natural and legal persons providing services of virtual assets without registration, including the process of application of adequate sanctions.

It will be necessary to consider a modification of the system of sanctions in the AML Act as well as in the Criminal Code so that they will cover not only the providers of services of virtual assets but also their directors and top management.

The preparation of a Methodical Guide for the providers of services of virtual assets and its publication at the website of the FIU SR should correlate with the training of obliged entities in the AML area provided by the FIU SR. The objective of these tasks should be the setting of a suitable and efficient framework for the monitoring and reporting of these operations with virtual currencies, which could be potentially connected with crime.

Taking into account the specific character of a transaction with virtual assets often taking a fragment of a second in the online environment and having a transnational extent, it appears inevitable to set suitable and prompt communication systems between the FIU SR and obliged entities, as well as between the FIU SR and foreign Financial Intelligence Units.

In the context of the above-mentioned facts it is necessary to realise that UT identification by an obliged entity and its subsequent assessment by the FIU SR is only an initial entrance gateway of the whole investigation process, which would start quickly and efficiently immediately after a suspicion appears that the virtual assets concerned are connected with crime. As it is a new area, in relation to investigation, training of competent workers and preparation of methodologies facilitating and unifying the procedures of law enforcement authorities will also be necessary.

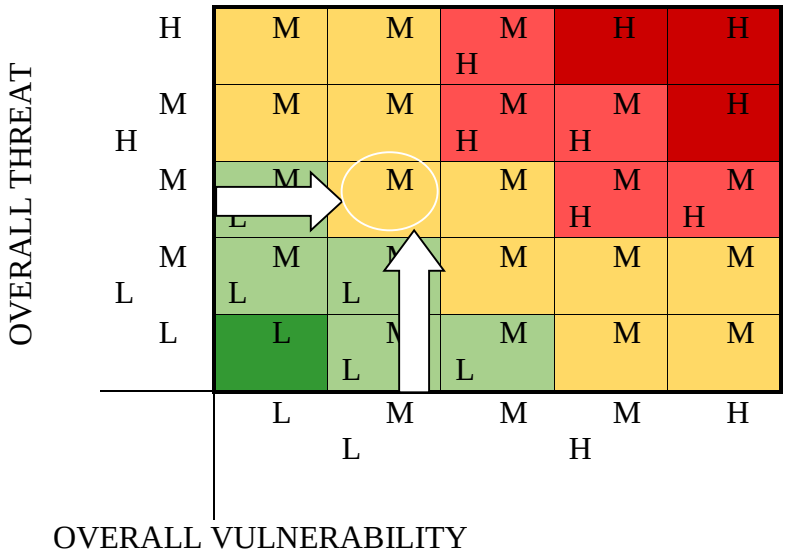
Search for virtual assets should be a standard part of financial investigation and search for property pursuant to a special act (Act No. 101/2010 Coll. on proving the origin of property).

Last but not least, it will be necessary to improve cooperation both at international and national levels, in particular between the FIU SR and other parts of the Police Force, as well as between the FIU SR and the National Bank of Slovakia, Ministry of Finance, Financial Administration, both in the area of mutual exchange of information, coordination of procedures, training of competent employees, and within the framework of coordinated approach to the building of general public’s awareness of the area of virtual assets.

7. TERRORIST FINANCING RISK

The overall RISK LEVEL for terrorist financing in the conditions of the SR is at a **MEDIUM** level.

Based on the assessment of gathered information and data, the overall level of THREAT of terrorist financing in the conditions of the SR was determined at **MEDIUM** level and the overall level of VULNERABILITY was determined at **MEDIUM-LOW** level.



Terrorism and the related extremism radicalisation are currently the most serious security threats for every country and its constitutional arrangements; therefore, they also represent the biggest challenges for state authorities. Therefore, efficient detection of various forms of terrorism already at an initial stage with the objective to prevent human casualties, protect material values or prevent the destabilisation of state pillars became a primary interest of States.

Procedures based on the methodology "FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment"[78] and the World Bank's methodology were used in the process of the 2nd assessment of the terrorist financing risk.

The FATF methodology mentions that the terrorist financing risk can be seen as a function of three factors: threat, vulnerability and consequence. Financial resources or other assets intended for a terrorist or terrorist organisation can be obtained, relocated, stored or used in a country or through a country in the form of legal or illegal funds or other assets.

[78] http://www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

Domestic sources of the terrorist threat

No presence or activities of any domestic Islamist or non-Islamist terrorist organisation were recorded in the territory of the Slovak Republic in 2016 - 2019. The terrorist threat from these organisations or lone actors and foreign fighters inspired by them was assessed as relatively low in the period. Neither the establishment of an Islamist or non-Islamist terrorist organisation in the territory of the SR nor a significant increase in the number of domestic self-radicalised individuals willing and able to commit a terrorist act in the territory of the SR is expected in the near future.

No terrorist attack was carried out in the SR in the monitored period. The terrorist threat in the territory of the SR is primarily affected by the external environment, in particular the security situation in some Member States of the European Union (EU), which are confronted with both successfully completed, as well as frustrated terrorist attacks and individual violent incidents committed by followers of international jihad inspired in particular by the jihadist propaganda in social media.

The radically-thinking individuals' existence and effect on the organisations presenting far-right ideology, on the organised crime or States with undemocratic political regime belongs to the basic potential domestic terrorist threats.

Potential returnees from conflict regions, where foreign fighters operate (Syria, Iraq, Ukraine), can also represent an increased security threat to the SR. The obtained experience in fights, experience in violent forms of achieving the set goals, as well as, for example, knowledge of explosives handling can become a basis of terroristic methods, asocial behaviour or building personal authority in the structures of extremist groups. Potential risk can also be represented by contacts with risky persons obtained abroad. Only sporadic cases of activities of citizens or foreigners with the residence in the SR in conflict zones in the Middle East were recorded during the assessed period. As regards the identification of foreign fighters, intelligence services are preferably focused on the detection of the method of travelling and funding of travelling and the stay in the target country including the monitoring of movement in the country with respect to a possible return to the SR or to the Schengen area.

Cases of interconnection of Slovak Muslim community members with radical representatives of Muslim communities from the neighbouring EU Member States (the Republic of Austria, Czech Republic) were recorded in the assessed period.

Open sources contain information concerning the activities of a radical Imam, who worked in Prague and in one of the houses of worship in Bratislava. In 2016, he allegedly helped one person coming from the Republic of the Sudan with residence in the SR travel to Syria with the objective to join jihadists. In addition to the above man, he also helped his brother with wife travel to Syria with the objective to join the jihadist group Al-Nusra Front (currently known as HAY'AT TAHRIR AL-SHAM, HTS)[79].

[79] The High Court in Prague imposed a sentence of imprisonment for a term of ten years upon the Imam for the participation in a terrorist group in the form of assistance

A case of a radicalised SR national was also publicised in media in connection with the Czech Republic. In December 2018, he was indicted for the preparation of a terrorist attack and promotion of a movement leading to the repression of human rights and freedoms. In 2019, he was convicted of endangering public safety[80].

Further, a case is known, when a citizen of Israel staid in the territory of the SR from 2016 for the purpose of studying at a university and in July 2019, he was arrested in Israel and accused of the preparation of a terrorist attack and support of the Islamic State by disseminating radical ideology via the internet and by creating fake internet profiles for other fighters.

The popularity, influence and capacities of paramilitary groups increased in the SR in the assessed period. A more significant shift or inclination of the value orientation of come paramilitary groups towards the far-right ideology, radicalisation of their members and possible participation in the activities connected with the support of terrorism and terrorist financing and other activities related to terrorism cannot be excluded in the long term.

Four criminal prosecutions connected with criminal offences of terrorism were commenced in the assessed period, however, nobody was charged. It is necessary to emphasise that in the cases of criminal proceedings for criminal offences of terrorism, also financial aspects of these acts were investigated, including the detection of possible resources helping commit the criminal offences. The examination or investigation especially determined whether also other people in addition to the perpetrator took part in the commission of any of the criminal offences, in particular in the form of help or direct or indirect financing of their activities including the provision of the essentials of living.

In 2018, one citizen of the SR was indicted for a particular serious criminal offence of terrorism and some forms of participation in terrorism pursuant to Article 419 of the Criminal Code and the criminal offence of illicit manufacturing and possession of nuclear materials, radioactive substances, hazardous chemicals and hazardous biological agents and toxins pursuant to Article 298 of the Criminal Code. He committed the above criminal offences by sending mails to various state institutions, which contained a radioactive substance and a threatening text. In 2019, the Supreme Court of the SR requalified the act to a particularly serious crime of endangering public safety pursuant to Article 284 of the Criminal Code at a stage of an attempt and a minor offence of an attack against a public authority pursuant to Article 322 of the Criminal Code in concurrence with the minor offence of spreading an alarming news pursuant to Article 362 of the Criminal Code[81].

Based on the results of competent authorities in obtaining and evaluating knowledge and information about possible or potential security threats to the Slovak Republic and its citizens in the territory of the Slovak Republic, it can be assessed that the overall threat of a terrorist attack by domestic actors was assessed as **LOW** in the period under assessment.

[80] In 2020, the High Court of Appeal in Prague imposed a sentence of imprisonment for a term of five years upon a citizen of the SR for the promotion of a terrorist organisation

[81] In 2020, a cassation appeal was filed in the case – the judgement is not final

Regional sources of terrorism threat

In the monitored period, the influence of regional Islamist, non-Islamist terrorist organizations, lone actors or foreign fighters inspired by them was not recorded in the territory of the Slovak Republic.

A growing level of terrorist threat has been identified in Austria, where several attempts at terrorist attacks by lone attackers and returnees from conflict zones have been thwarted in the last two years.

Ukraine, as another of the immediate neighbours, has been marked by an ongoing armed conflict since 2014. Nevertheless, the security situation in Ukraine alone does not pose a primary threat of terrorism. The conflict in the south-east of Ukraine can be considered internal in terms of borders. However, the consequences of this conflict may secondarily pose a threat to the Slovak Republic in the following areas:

1. The weakened or underfunded state administration of Ukraine is not able to ensure effective control of the state border, both at entry and exit. This can be exploited by human smuggling and smuggling groups to infiltrate people (including people from high-risk countries with possible personal ties to terrorist groups) and goods into the EU territory.
2. The uncontrolled movement of weapons and explosives in the context of a conflict is an easily accessible commodity for organised and criminal groups as well as individuals. This acquired material can then be exported to EU territory through smuggling channels and misused by terrorist groups.
3. Fighters from third countries, including countries / regions of Islamic faith, who formed separate battle groups, also took part in the fighting in south-eastern Ukraine. These persons, on the basis of the Ukrainian law "On the Legal Status of Aliens and Stateless Persons Who Participated in the Protection of the Territorial Integrity and Integrity of Ukraine", may be granted Ukrainian citizenship, which will make it easier for them to travel to EU countries in the future.

In the regional context, several sources of threats of Sunni terrorism were indicated (both real and potential), with links to the Western Balkans in particular. The real threats of terrorism are linked to the uncovered planned attacks in the Western Balkans. Several security actions of security forces against Islamic radicals took place in the region, confiscating weapons and various equipment needed to plan and commit a terrorist attack.

In particular the return of foreign fighters and their family members and spreading radical Islamist ideologies (Salafism and Wahhabism) should be mentioned as potential threats.

In addition to the Western Balkans region, there was an increase in the popularity of Salafism and its membership in some EU countries with a stronger Muslim population. The threats of terrorism related to the movement of high-ranking or particularly dangerous persons with ties to the ISLAMIC STATE and other jihadist groups in the territory of some countries neighbouring the Slovak Republic, including EU Member States, were also identified in the period under assessment. In recent years, the so-called sources of domestic terrorism have been

evaluated in the EU (terrorism that originates directly in EU countries, not abroad), with communities of less integrated second-generation immigrants from the Middle East and communities of European converts to Islam being identified as risky. Communities of right-wing and left-wing extremists and ethnic separatists have also been identified as risky.

During the period under assessment, the planned release of those convicted of terrorist offenses appeared to be a potential source of threat in some EU Member States. These people may continue to pose a threat even after their release, due to their expected continued radicalisation and the problem of their subsequent comprehensive monitoring. At the end of the period under assessment (29 November 2019), a terrorist attack was carried out in London by Usman K. inspired by the propaganda of the jihadist group AL-QAEDA, who was prematurely released from prison in December 2018.

Based on the results of competent authorities in the field of obtaining and evaluating knowledge and information about possible or potential security threats to the Slovak Republic and its citizens in the territory of the Slovak Republic, it can be assessed that the overall threat of a terrorist attack by regional actors was assessed as **MEDIUM-LOW** in the period under monitoring.

Global sources of terrorism threat

An indirect influence of global Islamist and non-Islamist terrorist organisations was recorded in the territory of the SR in 2016 - 2019. Under the influence of propaganda of such organisations, several individuals travelled to conflict zones; isolated cases of individuals sharing jihadist materials on social networks were also identified.

In the media propaganda of Islamist terrorist organisations in the period under assessment, the Slovak Republic was named as part of the anti-terrorist coalition of Western countries and described as an "enemy of Muslims".

In the period under assessment, there has been a shift in the modus operandi of terrorist attacks abroad. Gradually, the level of sophistication of attacks decreased with the onset of a simple method of attack without longer, complicated preparation with easily accessible means, at minimal financial cost to soft targets in publicly available and frequented places. Most of the terrorist attacks were carried out by lone actors / small groups, the attackers were young second- and third-generation Muslims from North Africa, the Middle East and the Caucasus, with no combat experience, motivated by Islamist extremist references on the Internet, or influential people (e.g., Imams). In this context, it should also be emphasized that in 2018 there was a significant decrease in the number of successfully carried out Islamist-motivated terrorist attacks in Europe (22 in 2017 and 8 in 2018) - especially by the jihadist organisation ISLAMIC STATE. This fact was determined by a combination of an increase in the number of thwarted terrorist attacks in Europe (from 8 in 2017 to 17 in 2018), successful security interventions and the severely limited capabilities of the ISLAMIC STATE. The declining trend of terrorist attacks continued in 2019.

Global terrorism remains the biggest security threat, with an impact on the security situation in the Slovak Republic and the interests of the Slovak Republic, or NATO and the EU.

Threats in this context continue to stem mainly from global terrorist or jihadist groups such as ISLAMIC STATE and AL-QAEDA and their regional branches. It is likely that the further development of terrorism and jihadism in the world will be determined at least in the near future by the activities and capabilities of the ISLAMIC STATE and AL-QAEDA. It is also likely that the current dynamics of armed conflicts and the evolving socio-economic situation in the Middle East and the Maghreb and Sahel will further stratify the sources of regional threats in the near future with the potential to worsen the global security environment.

In the emergence and expansion of terrorist groups on a global scale, the so-called failed states have a significant share. The high vulnerability of their internal security environment is exploited by various state and non-state actors, including militant and terrorist groups, to advance their own interests. The support of terrorism by various, especially authoritarian regimes, which financially, materially, ideologically and in other ways support movements and persons promoting their interests abroad, is also closely connected with the issue of failing states.

Another global security threat (even in the context of the long-term time horizon) is the education of the second generation of jihadist fighters. The actors of global terrorism are targeting this phenomenon and the failure to address the situation of detained ISLAM STATE fighters and their families in prisons and internment camps in the Middle East also contributes to this phenomenon.

Propaganda is an important and effective tool for the spread of jihadism and for achieving terrorist, conventional-military and non-military goals of individual terrorist or jihadist groups. The most significant propaganda activity in recent years has been carried out by the ISLAMIC STATE. It Primarily uses propaganda as part of its military efforts to achieve the strategic goal of establishing a caliphate, which involves the recruitment of new fighters, influencing the local population[82], intimidating the enemy, inciting and instructing individuals to make terrorist attacks in their home countries, etc. The ISLAMIC STATE makes extensive use of multilingual media production and propaganda and has numerous media agencies or entities that are either a direct part of it or are strongly pro-IS oriented. The media products that these entities create are most often documents, videos and magazines. In the assessed period, they mainly used the online environment for their dissemination, especially social networks and various communication applications. At the end of the period under assessment, there was an increase in the activities of support groups in this context. Other jihadist and militant groups, such as AL-QAEDA or the HTS, also carry out propaganda activities. AL-QAEDA has long promoted the idea of uniting all Muslims within one world community (ummah) into a form of state (by the gradual spontaneous integration of Muslims) that would live in accordance with Islamic Sharia law.

[82] Propagandistic activities of the IS, which are focused on the recruitment of new fighters and influencing the local population, show signs of using the methods of sectarian groupings, when the propaganda offers, inter alia, the way out of seemingly hopeless life situations. Groups offer a haven of rest where an individual is welcome and needed, thus creating an impression that by joining the group, the individual will fulfil their need (reason for existence) or desire to belong somewhere (be part of something) and will not remain on the margin of society or miss opportunities for some form of self-fulfilment.

The threat of terrorism against the Slovak Republic in the wider geopolitical area is also posed by the Slovak Republic's involvement in international crisis management operations and active involvement in the fight against terrorism. This fact in itself carries an inherent risk of retaliatory terrorist attack. The threat to the security environment of the Slovak Republic and the EU is also posed by migration from high-risk countries to EU countries, or a complicated process of integration of received asylum seekers in the Slovak Republic. Migration can be misused by supporters of terrorist groups to move safely to EU countries.

Based on the results of the competent authorities in obtaining and evaluating knowledge and information about possible or potential security threats to the Slovak Republic and its citizens in the territory of the Slovak Republic, it can be assessed that the overall threat of a terrorist attack by global actors was assessed in the period under monitoring as **MEDIUM-LOW**.

Degree of threat to the SR

The second (increased) degree of terrorist threat has been in force in the Slovak Republic since 23 August 2017. It has increased due to the deteriorating security situation in Europe. For jihadist groups, the Slovak Republic remains a secondary target compared to the western EU countries, where several terrorist attacks of various scales were carried out during the period under assessment.

Overall evaluation of terrorist threat in the territory of the SR

Based on the above facts, measures (countermeasures) taken by the competent authorities, the quality of legislation in the application of operational and procedural acts, the level of national and international cooperation and also with regard to the geographical location of the Slovak Republic it can be stated that the overall level of terrorist threat against the SR is **MEDIUM-LOW**.

In the 1st NRA, the overall level of terrorist threat to the SR was evaluated as low. The increase in the level of the threat to a medium-low was mainly influenced by security incidents with a terrorist background carried out within the geographical area of the EU, which were not directly related to the SR, but were reflected in the assessment of the appropriate degree of terrorist threat in the territory of the SR. In the assessed period of the 2nd NRA, a deterioration of the security environment in the EU was recorded.

Evaluation of terrorist FINANCING risk

In the SR, three cases of terrorist financing were recorded in the period under assessment, in which, however, no criminal prosecution was conducted against a specific person.

In the period under assessment, no Slovak citizens or foreign nationals were convicted in the Slovak Republic for financing terrorism or financing foreign terrorist fighters.

The 2nd NRA was targeted to sectors, which were used in the SR for acquisition and transfer of funds intended for terrorist support. The working group also focused on a **more comprehensive assessment of the non-profit sector**.

Case 1

Through other people, a religious leader (Imam) obtained financial resources in the territory of the SR and the Czech Republic in 2015 to 2017 in the form of fundraising for the construction of water pumps, however, the money obtained was subsequently used for the needs of people who travelled abroad and then, as members of terrorist groups, actively became involved in combat operations in the territory of Syria and Iraq. During the investigation it was found out that the funds collected through "fundraising" from worshippers were gathered on bank accounts of suspicious persons, from which they were withdrawn and either sent in cash through couriers to the addressees fighting in Syria or directly used for travelling costs of such people travelling to Syria and Iraq and to fulfil their needs – accommodation, equipment, food, etc. The people, who provided gifts in the territory of the SR, were heard and it was found out that they had known nothing about the real place of destination and use of financial resources. During the investigation, one particular person was identified – M. H., who travelled with the money to Syria, joined a terrorist group "AL-NUSRA FRONT" and participated in its activities. M. H. was killed during fights at the end of 2018. In this case, no preliminary measures were taken because the Imam had no property in the territory of the SR.

As it is obvious from the description, the criminal prosecution against the Imam was also led in parallel in the Czech Republic. For that reason, both Czech and Slovak authorities agreed upon coordination with the objective to solve the conflict of jurisdictions and eliminate the problem by applying the principle "ne bis in idem". The Imam was convicted in the Czech Republic and Slovak authorities subsequently made decision on the termination of criminal prosecution in the territory of the SR.

Case 2

An unidentified group of persons from the territory of the Slovak Republic sent several payments in various amounts via the Western Union service at least during 2016 to persons who directly or through other persons participated in the commission of various terrorist criminal offences, including membership in a terrorist organisation, and in this connection sent several amounts in particular to XY, who committed a terrorist attack in Istanbul on 1 January 2017, where he was detained by members of the Turkish security forces.

The investigation requires relatively demanding international cooperation with the judicial authorities of several countries outside the EU. It aims to identify all those who were directly or indirectly involved in the sending of money, to identify the total amount of funds as well as individual amounts, and to identify all persons to whom the funds were allocated, including their share in other terrorist offences. The case is still under investigation.

Case 3

The third case began in 2019 as part of a comprehensive investigation into other (serious) crimes. In the period 2013-2016, the person XY was to transfer funds from the bank account of company A kept in a Slovak bank to his own bank account opened in the same bank. Subsequently, the alleged perpetrator was to use these funds to support the terrorist organization X. The funds were transferred to the account of company A from the account of the foreign organization Y. An extensive financial investigation is still ongoing in this case, which has been extended to other companies linked to the alleged perpetrator.

The **following risk sectors** have been identified in relation to the terrorist financing cases described above:

- cash transport sector,
- sector of payment services, agents of payment services,
- banking sector:
  - ✓ cash operation on bank accounts,
  - ✓ cashless transfers of financial resources on bank accounts.
  - ✓

Sector of transport of cash

Threat-medium level

In the global context, the level of the threat of terrorist financing in relation to cash couriers is considered to be very significant. Terrorist groups repeatedly use cash couriers to fund their activities or to fund the travel of foreign terrorists. The risk of cash smuggling is particularly significant for couriers transferring cash from EU countries to third countries. The modus operandi of cash couriers was used in the first case of terrorist financing described above.

The effectiveness of cash transport control processes depends on the staffing and technical equipment of a particular border crossing point. Due to the geographical location of the Slovak Republic, the focus of control is on the eastern border (road, rail and passenger transport) and at international airports, especially Bratislava and Košice. The performance of control is based on the application of risk analysis by targeted selection of risk persons and their control, which is conditioned by an adequate level of training of customs officers in the form of courses in detecting smuggling, including smuggling of funds. Technical means such as X-rays, a service dog for searching for funds, premises intended for thorough customs control of means of transport, luggage are used to reveal the transported cash. In case of suspicion of a breach of customs regulations, the person is subjected to a security check, and in a justified case also to a personal check.

In the case of transport of funds in cash across the external borders of the Slovak Republic above the specified amount of EUR 10,000, if such transport is found, while the natural person transporting funds has not fulfilled the reporting obligation, it is a customs delinquency, which is solved by the Customs Office in accordance with Customs Act No. 199/2004 Coll. If, in connection with this transport, a criminal offence were suspected, the department competent to proceed with it would be the department according to the material area, i.e.:

a) the FACO in the investigation of criminal offences committed in connection with the violation of tax regulations in the field of value added tax on importation and excise duties or customs regulations, or
b) materially and locally competent PF department according to the regulation of the Minister of Interior of the Slovak Republic on defining the competence of PF departments and units of the MI SR in detecting criminal offenses, identifying their perpetrators and proceeding in criminal proceedings No. 175/2010.

The Financial Administration of the Slovak Republic evaluates the data declared on the preliminary customs declarations when performing a security and protective analysis of the risk related to the entry of goods into the customs territory of the EU and the exit / export of goods from the customs territory of the EU. The presented data is the basis for automated analysis of individual common risk criteria for entry, exit and export of goods. Verification of the riskiness of economic operators, countries, goods, vehicles, invalid documents is performed on data sources, which also include lists of restrictive measures:

- European Union Consolidated Financial Sanctions List https://webgate.ec.europa.eu/europeaid/fsd/fsf,
- Iran's nuclear weapons database https://www.iranwatch.org/.

The customs authorities of the SR are obliged to send the completed forms and notifications of violations of the customs regulations to the FIU SR by the fifth day of the calendar month following the month in which these facts occurred. In the SR, all notifications are submitted using a dedicated form, which is used by most EU Member States, the so-called CDF. The natural person makes the declaration in three copies (one original and two copies), of which the original is intended for the border customs office, the first copy is intended for the declaring natural person and the second copy of the declaration is sent to the FIU SR. If the conditions in terms of the obligation to declare pursuant to Article II (2) of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council are not met, or the data in the received declaration is incorrect, false or incomplete, the natural person is obliged to correct or complete the data. If the customs officer finds a non-compliance with the obligation to declare, the natural person shall additionally fill in the CDF form, on which the customs officer shall indicate in paragraph 7 in the "Official records only" section that it is a record and also indicate the sanction imposed. The border customs office shall draw up a report on the breach of customs regulations in the event that it does not resolve the breach by a fine on the spot.

In the assessed period, the FIU SR received a total of 770 declarations from the customs authorities of the SR in the total amount of EUR 37,034,757.58. A total of 156 customs declarations were lodged at international airports, in other cases the EU land border between the SR and Ukraine was used. The obliged entities were in most cases citizens of Ukraine, Hungary, and Russia. The most common purpose of using the transported cash, which the obliged entities declared mostly as their own savings, was the purchase of a car / truck, the purchase of real estate, a deposit in a bank account, business, personal need.

Summary of cash transport declarations

Year	Total number of cash transport declarations	Amount of transported funds in EUR	Number of fines imposed /total amount in EUR	Dissemination			
				KIS FIU SR	Foreign FIU	FD SR	PF dpt.
2016	124	4,016,396.51	7/875.00	102	42	15	-

		+ 1 bond in the amount of USD 25,000,000.00					
2017	152	5.261.245,86 + 1 bond in the amount of USD 14,975,000,000.00	16/1,671.00	134	14	1	-
2018	230	8,131,825.21	23/2,030.00	176	40	19	7
2019	264	19,625,290.00	19/1,350.00	211	55	6	-

Summary of cases and the amount of fines imposed by Customs Offices

	Number of cases/the amount of fine in EUR			
	Year			
Customs Office	2016	2017	2018	2019
Banská Bystrica	2/100.00	-	1/100.00	-
Bratislava	-	-	2/30.00	-
Košice	2/1,200.00	-	1/150.00	-
Michalovce	14/1,600.00	7/400.00	7/140.00	6/270.00
Nitra	-	-	14/330.00	20/128.00
Prešov	1/0	1/300.00	-	1/50.00
Trenčín	2/600.00	5/530.00	1/250.00	3/100.00
Trnava	-	-	-	2/310.00
Žilina	-	-	-	65/4,240.00
Sum total	21/3,500.00	13/1,230.00	26/1,000.00	97/5,098.00

Vulnerabilities:

- no legislative coverage of transport of cash by freight transportation and postal consignments
- no system for declaring cash at EU internal borders
- no obligation to report under-limit cash (smurfing)
- the sanctions for non-declaration or misdeclaration are not sufficiently dissuasive
- the absence of adequate legislative and organizational measures to effectively seize suspicious funds
- declaration forms are submitted to the FIU SR only once a month (specifically only in the calendar month following the month in which the funds were transported)

Vulnerability - medium level

Sector of payment institutions, payment service agents and electronic money institutions

Threat - medium level

In connection with the 2nd case of terrorist financing described above, a group of persons was identified who, through the Western Union service, sent payments to persons who were directly or through other persons involved in the commission of various terrorist offences. The investigation in this case is still ongoing and it is not possible to draw a relevant conclusion (proving intentional conduct). However, it has undoubtedly been identified that the sector in question is at risk of raising funds and transferring funds to support the financing of terrorist activities.

A payment institution is a legal person which is, on the basis of a permit granted by the NBS pursuant to Act No. 492/2009 Coll. on payment services authorised to provide payment services without restriction or to a limited extent, while at least one payment service according to the granted authorisation must be provided in the territory of the SR. A payment institution that has the permission of another competent national authority in the European Economic Area may also provide its services in the SR.

A payment institution may provide payment services through a payment service agent. The payment institution is obliged to notify the NBS of this intention. After the legal conditions have been met, the NBS will enter the payment service agent in the list of payment service agents. Agents registered in other EU Member States can provide payment services in the SR if the NBS receives the relevant notification from the supervisory authorities in the given states. The current list of agents of payment institutions is published by the NBS on its website. The provision of Article 70 of Act No. 492/2009 Coll. on payment services obliges the payment institution to develop and maintain an effective internal control system. For the purposes of the said Act, internal control is considered to be control of compliance with laws and other generally binding legal regulations, the statutes of the payment institution, prudential rules and protection against money laundering and terrorist financing.

An electronic money institution is authorised to issue, manage electronic money and perform payment operations. An authorisation from the NBS is needed for its activity. Pursuant to the provision of Article 82 (4) of Act No. 492/2009 Coll., the application for the authorisation to issue electronic money is accompanied, inter alia, by a draft of internal rules governing the electronic money institution’s internal control management mechanisms, including risk management procedures and internal rules governing AML / FT mechanisms.

Obliged entities for the financial sector pursuant to Article 5 (1) of the AML / CTF Act include, inter alia, payment institutions, payment services agents and electronic money institutions. The fulfilment and observance of obligations of obliged entities established by the AML / CTF Act is controlled by the FIU SR. The sector is also subject to financial supervision by the NBS.

The principle of providing payment services did not change in the period under assessment. The method of providing payment services is subject to change, which changes depending on the speed of development of financial innovations. Modern technologies enabling remote communication and identification and verification of identification come to the fore, as

well as new applications enabling the use of payment services quickly and securely without personal participation.

Based on the evaluation of information and data obtained within the process of the 2nd NRA it can be stated in general that entities in this sector do not pay sufficient attention to the risks associated with terrorist financing. Most entities use a manual monitoring system. Entities monitor persons on sanction lists, but do not have a sufficient frequency of monitoring the business relationship. There is no monitoring of the business relationship of existing customers.

Sector size

Year	Payment institution	Agents of payment services	Electronic money institution
2016	2	19	1
2017	2	17	1
2018	9	14	1
2019	10	16	1

Summary of received reports from payment institutions, payment service agents and electronic money institutions

Year	Number of UTRs
2016	38
2017	31
2018	24
2019	27

The FIU SR in the period of 2018 - 2019 also received information from foreign payment institutions operating in the Slovak Republic in the total number of 552. The analysis of individual information revealed that these institutions were used mainly for transfers of funds in the order of hundreds to thousands of euros to high-risk countries Syria, Iraq, Iran, Benin, Togo, Oman, Nigeria, Burkina Faso, while the connection with the Slovak Republic was identified through the subject of the sender or recipient of payments. A network of agents in different countries was used. The problem seems to be to obtain all available information on financial flows, due to the different legal regulation of data provision in foreign jurisdictions. Where relevant, the information was forwarded for further verification by the competent authorities of the Anti-Terrorism Centre NAKA, SIS.

In the assessed period, the FIU SR performed 2 inspections in the mentioned sector and the NBS performed 6 on-site inspections.

A detailed analysis of the sector of payment institutions, payment service agents and electronic money institutions is provided in the section “sector of other financial institutions”.

Vulnerabilities:

- use of products without personal presence
- fast transfers of funds across several countries (even high-risk ones)

- easy availability of payment service agents
- wide intermediary network and simplicity of the product
- weak knowledge of the sector about the obligations with regard to FATF Recommendation R16
- insufficient surveillance - low number of controls

Vulnerability - medium-low level

Banking sector

Threat - medium level

Cash deposits in accounts can be used by terrorists due to the simple depositing of cash in bank accounts and the subsequent withdrawal of funds. The risk scenario was used in the first described case of terrorist financing, where funds collected through "fundraising" were accumulated in the bank accounts of suspects, from where they were withdrawn and then sent to combatants in Syria, or were used directly for travel expenses of such persons travelling to Syria and Iraq and to ensure their needs - accommodation, equipment, food, etc. Payment services allow cross-border transactions to take place and, depending on the specific national legislation, different means of identification may be used.

The banking sector in the period under assessment consisted of 27 banking entities, with 9 banks, 14 branches of foreign banks, 3 building savings banks and 1 savings and credit cooperative, an organisational unit of a foreign entity. Cooperation with the banking sector is crucial from the point of view of the AML / CTF Act, given the number of customers, the scope and volume of processed transactions. The banking sector is most active in taking measures to mitigate FT risks and is also most involved in reporting UTs. Weaknesses were identified in the application of due diligence measures, in particular in the area of verifying the origin of funds or assets in a business or business relationship.

Cash operations on bank accounts

In connection with cash transactions, the bank's employees are obliged to identify the depositor and his relationship with the account holder, determine the origin of funds depending on ML / TF risk, the purpose of the transaction, ownership of funds regardless of the transaction amount and acting on their own behalf through a written declaration, etc. Cash transactions pose a risk of interruption of financial flow monitoring and continuity, as well as a risk of placing illegal money in the legal financial system. Approximately 20% of banks use ATMs with a deposit function. Banks have taken several measures to mitigate the risks with the mentioned product, for example: analysis of possible risks, especially with regard to the type of customer, the introduced limit for cash deposits via ATM, increase of limits for ATM deposits is approved by the Compliance and AML Department, customers can make cash deposits via ATM only into their own account, deposits via ATM are monitored by the AML department, in case of suspicion, customers must declare the origin of funds.

Cashless payment transactions and electronic banking

Before providing a product to a customer, banks thoroughly verify the customer and obtain necessary information within due diligence. On the other hand, in the case of these products, risks related to the characteristics were identified, in particular the possibility of carrying out unlimited transactions, including transactions to risk areas.

Banks use specific scenarios and management models in managing risks related to terrorist financing, and their essence lies in assessing, in particular, geographical risks. In the case of non-residents, they assess the justification for opening accounts in the Slovak Republic. An important part of the process is also the monitoring of transactions - especially to / from high-risk countries, verification of sanction lists.

A detailed analysis of the banking sector is provided in the part "banking sector".

Vulnerabilities:

- efficiency of cash transactions monitoring
- unlimited number of cash and cashless operations
- insufficient surveillance - low number of controls

Vulnerability – medium-low level

Non-profit sector

Threat – medium-low level

The threat of terrorist financing in connection with the use of funds through the non-profit sector appears to be globally unused by terrorist groups. In rare cases, however, the non-profit sector may be abused by terrorists, especially in relation to the financing of foreign terrorist fighters, which may then pose a significant threat. In the assessment period, no cases of the use or misuse of the non-profit sector for terrorist financing were detected in the Slovak Republic.

In the 5th round of evaluation of the Slovak Republic, the MONEYVAL Committee of Experts evaluated the non-profit sector partly in accordance with the FATF recommendation (R.8), in particular criticizing that the 1st NRA did not contain the identification of characteristics and types of non-profit organisations (hereinafter "NPOs"), for which, based on their activities or features, there could be a risk of their abuse for terrorist financing. In view of the above, the non-profit sector was subjected to a more comprehensive analysis in the 2nd NRA.

FATF defines non-profit organisations as "a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". This definition is based on those activities and characteristics that expose non-profit organizations to the risk of misuse for terrorist financing.

In the conditions of the SR, the following organisations can be identified in compliance with the FATF definition:

- **foundations** (Act No. 34/2002 Coll. on foundations and on the amendment to the Civil Code),
    - foundation is a special-purpose non-investment pooled asset fund that serves to support a public benefit purpose,
    - a public benefit purpose in this case means, in particular, the development and protection of spiritual and cultural values, the exercise and protection of human rights or other humanitarian objectives, the protection and creation of the environment, the preservation of natural values, health protection, the protection of children's and youth rights, development of science, education, physical education and the provision of individually designed humanitarian aid for an individual or a group of persons who have found themselves in danger of death or in need of urgent assistance in the event of a natural disaster,
- non-profit organisations providing welfare services (Act No. 213/1997 Coll.),
    - a non-profit organisation is a legal person providing welfare services under equal conditions for all users specified in advance and whose profit cannot be used in favour of founders, members of bodies or employees; it must be fully used to provide for welfare services,
    - welfare services in this case are in particular the provision of health care, the provision of social assistance and humanitarian care, the creation, development, protection, restoration and presentation of spiritual and cultural values, the protection of human rights and fundamental freedoms, education, training and physical culture, research, development, scientific-technical services and information services, creation and protection of the environment and protection of the health of the population, services to support regional development and employment, provision of housing, administration, maintenance and renewal of the housing stock,
- **non-investment fund** (Act No. 147/1997 Coll.),
    - the fund is a non-profit legal person that brings together funds intended for the fulfilment of a public benefit purpose or individually determined humanitarian aid for an individual or a group of persons who have found themselves in danger of life or need urgent assistance in the event of a natural disaster,
    - a public benefit purpose means, in particular, the development and protection of spiritual values, the protection of human rights, the protection and creation of the environment, the preservation of natural and cultural values, the protection and promotion of health and education, the development of social services,
- organisations with an international element (Act No. 116/1985 Coll.),
    - an organisation with an international element is an international non-governmental organisation and an organisation of foreign nationals,
- **church legal persons** (Act No. 308/1991 Coll.),
    - a church or religious society is a voluntary association of persons of the same religious faith in an organisation formed according to affiliation to a religious faith on the basis of the internal regulations of the relevant church or religious society,

- **associations** (associations, societies, unions, movements, clubs and other civic associations, as well as trade unions – Act No. 83/1990 Coll.),
    - citizens have the right to associate freely – Article 29 of the Constitution of the SR 460/1992 Coll. guarantees the right to associate freely. Everyone has the right to associate with others in associations, societies or other unions,
    - no permission of a state authority is necessary to exercise this right.

In accordance with Act No. 297/2008 Coll. on the protection against the legalisation of proceeds of crime and terrorist financing (hereinafter the "AML/CTF Act"), pursuant to Article 9 (e), pooled asset funds mean foundations, non-profit organisations providing welfare services, non-investment funds or other special-purpose pooled asset funds regardless of their legal personality, which administer and distribute financial resources. The AML/CFT Act imposes duties upon pooled asset funds (Article 25 (1)) – to identify the donor and natural person or legal person provided with financial resources by the pooled asset fund, if the value of the gift or the amount of provided funds exceeds at least EUR 1,000.00. The FIU SR is authorised to carry out a control in the pooled asset fund for the purpose of identification of the beneficial owner and verification of veracity and completeness of data on beneficial owner, identification of persons pursuant to Section 1 or for the purpose of verification of assets disposal.

Measures supporting the transparency of non-profit sector

Act No. 346/2018 Coll. on the register of non-governmental non-profit organisations (hereinafter "NGNPOs") came into effect on 1 January 2019. The objective of this act was to establish a reliable, up-to-date and uniform source register of NGNPOs registered with the Ministry of Interior of the SR ("MI SR"). The register of NGNPOs will represent a uniform source of data on:

- civic associations,
- trade unions,
- employer organisations,
- organisations with an international element,
- non-profit organisations providing welfare services,
- foundations,
- non-investment funds.

The register will be in the form of an open register which will also enable the registration of data on organisational units of NGNPOs or other legal persons. The original source registers will be cancelled and data from them will be migrated automatically. Individual registers are kept by the MI SR and they are publicly available. The register of NGNPOs will be put into operation on 1 January 2021.

Pursuant to Article 3 of Act No. 346/2018 Coll. on NGNPOs, the following data is registered in the register – name, registered office of the registered person; ID number; legal form; identification data on the natural person or legal person being the founder or member of the preparatory committee; identification data on the natural person, who is the statutory body.

If a non-profit organisation providing welfare services, non-investment fund or foundation is concerned, the identification data on beneficial owner and data establishing the position of beneficial owner is recorded in the register. From the register of NGNPOs, data on beneficial owners is provided to the Register of Legal Persons, Entrepreneurs and Public Authorities. The register will also contain the electronic form of statutes, founding charters, founding contracts, foundation documents and amendments to them. The register will have public part and a non-public part.

Pursuant to Article 6 of Act No. 346/2018 Coll. on NGNPOs, if the registered person fails to provide all the required data, the general government entity must not provide it with public finances, and the person must not acquire the State's property, the property of a higher territorial unit, municipality or public institution.

Before registering a legal person, the competent register authority (foundations – MI SR, non-profit organisations providing welfare services and non-investment funds – district offices) checks the integrity of the statutory body through the Oversi portal, by requesting an abstract of criminal records from the General Prosecutor's Office of the Slovak Republic. After the registration, the competent register authority controls the entities in compliance with the applicable generally binding legal regulation by evaluating the Annual Reports (in accordance with Article 37 (1) of Act No. 34/2002 Coll. on foundations and on the amendment to the Civil Code as amended, in accordance with Article 35 (1) of Act No. 213/1997 Coll. on non-profit organisations providing welfare services and Article 26 (1) of Act No. 14/1997 Coll. on non-investment funds). The entities are obliged to save their Annual Report in the public part of the Registry of Financial Statements (hereinafter the "Registry") by 15 July of a calendar year. Pursuant to applicable legal regulations, a fine is imposed on foundations and non-profit organisations providing welfare services only for a failure to save the Annual Report in the Registry within the period specified by law or for saving it with delay (saving after the deadline specified by law). The Act on Non-Investment Funds does not contain a provision on the obligation to impose a fine for breach of the obligation to submit an annual report to the register. The register authority checks the content of Annual Reports, including the annual financial statements. The Annual Reports must contain certain legal requirements, in particular:

- non-profit organisations (Article 34 of Act No. 213/1997 Coll. on non-profit organisations providing welfare services):
    - an overview of the activities performed in the calendar year, indicating the relationship to the purpose of establishing a non-profit organisation,
    - the annual financial statements and the evaluation of the basic data contained therein,
    - an overview of cash receipts and expenditures,
    - an overview of the scope of proceeds (proceeds) broken down by sources,
    - the status and movement of assets and liabilities of the non-profit organisation,
    - changes and new composition of the bodies of the non-profit organisation that took place during the year,
    - the Annual Report must be filed in the public part of the Registry of Financial Statements and must be accessible to the public at the registered office of the non-profit organisation,

- foundations (Article 35 of Act No. 34/2002 Coll. on foundations):
  - an overview of the activities carried out in the assessed period with an indication of the relationship to the public benefit purpose of the foundation,
  - the annual financial statements, evaluation of the basic data included in it and the opinion of the statutory auditor on the annual financial statements,
  - an overview of proceeds (proceeds) broken down by sources and origin,
  - a list of donors if the value of donations or the amount of funds from the same donor exceeds EUR 331,
  - an overview of the natural and legal persons to whom the foundation has provided funds for the public benefit purpose for which the foundation was established and information on how these funds were used,
  - total expenses (costs) broken down into expenses according to individual types of activities of the foundation,
  - changes made in the foundation charter and in the composition of bodies that occurred during the evaluated period,
  - the Annual Report must be filed in the public part of the Registry of Financial Statements,

- non-investment fund (Article 25 of Act No. 14/1997 Coll.):
  - an overview of the activities carried out in the assessed period with an indication of the relationship to the purpose of the fund,
  - the annual financial statements and evaluation of the basic data included in it,
  - an overview of donations and contributions provided to the fund,
  - an overview of proceeds broken down by sources and origin,
  - the state of the fund's assets and liabilities as at 31 December,
  - total expenditures broken down into expenditures according to individual types of fund activities and especially the amount of expenditures for fund management,
  - changes made in the statute and in the composition of bodies that occurred during the evaluated period,
  - the Annual Report must be filed in the public part of the Registry of Financial Statements.

Statistical overview of the number of non-profit organisations and of fines imposed by the register authority:

Year	Number of active ones as at 31 Dec.	Number of new registrations	Number of erasures	Number of fines imposed	Total volume of fines
2016	1335	218	44	No statutory duty	-
2017	1479	149	49	161	EUR 8,325.00
2018	1611	134	36	151	EUR 11,730.00

2019	1696	85	29	Not assessed	-

Statistical overview of the number of foundations and of fines imposed by the register authority:

Year	Number of active ones as at 31 Dec.	Number of new registrations	Number of erasures	Number of fines imposed	Total volume of fines
2016	409	24	8	50	EUR 21,640.00
2017	434	25	7	40	EUR 13,985.00
2018	446	13	7	35	EUR 5,900.00
2019	470	24	7	Not assessed	-

Statistical overview of the number of non-investment funds:

Year	Number of active ones as at 31 Dec.	Number of new registrations	Number of erasures
2016	484	10	6
2017	490	6	28
2018	497	7	5
2019	510	13	5

The register authority for civic associations is the MI SR. The conditions for the establishment and legal status of civic associations are regulated by Act No. 83/1990 Coll. on the association of citizens as amended. Citizens can form and associate in associations, societies, unions, movements, clubs and other civic associations, as well as trade unions and employers' organisations. The right to freely associate with others in associations, societies or other associations is guaranteed by the Constitution of the Slovak Republic (Article 29). It further follows from Article 29 that that right may be restricted only in cases provided for by law if, in a democratic society, it is necessary for the security of the State, for the protection of public order, for the prevention of crime or for the protection of the rights and freedoms of others. Legal persons can also be members of an association. Associations are legal persons. They are established by registering. The application for registration must contain information about the statutory body of the association or members of the statutory body of the association. The proposal must be accompanied by the statutes, which must contain, inter alia, the objective of the activity and the principles of management. The register authority shall refuse registration if:

- it is a political party and a political movement, an organisation set up for gainful employment or to ensure the proper exercise of certain professions, or a church and religious society,
- the statutes do not comply with the act,
- it is an illicit association,
- the goals of the association are in conflict with the requirements of the act (Article 5).

Civic associations are not obliged under Act No. 83/1990 Coll. to prepare an annual report. This obligation arises only in the case of the audit obligation and in the provision of social services pursuant to Article 67a of Act No. 448/2008 Coll.

Number of registered civic associations in individual years:

Year	Number of new registrations
2016	2,480
2017	2,500
2018	2,630
2019	2,806
Total number of CA as at 31 Dec.2019	50,835

The register authority for organisations with an international element is the MI SR. The conditions on the basis of which an international organisation may be established, operate or have its registered office in the Slovak Republic are regulated by Act No. 116/1985 Coll. on the conditions of operation of organisations with an international element. For the purposes of this Act, an organisation with an international element is defined as an international non-governmental organisation and an organisation of foreign nationals. The application for a permit to operate in the SR must contain, inter alia, the subject of the activity to be performed in the territory of the SR, the name and address of the statutory representative of the organisation and its organisational unit. The application for a permit must be accompanied in particular by the statutes - the organisational rules and the content of the activities of the organisation. The Ministry of Interior, in agreement with the Ministry of Foreign and European Affairs of the Slovak Republic and in consultation with the relevant central government bodies, may authorise the establishment of an organisation with an international element or allow such an organisation to operate or have its registered office in the SR.

Statistical overview of the number of organisations with an international element:

Year	Number of active ones as at 31 Dec.2019	Number of new registrations	Number of erasures
2016	115	1	0
2017	116	1	4
2018	116	0	1
2019	117	1	0

The register authority for churches and religious societies is the Ministry of Culture of the SR (Act No. 308/1991 Coll. on freedom of religion and the status of churches and religious societies as amended). The application for registration is accompanied by a basic document of the founded church or religious society (statute, order, statutes, etc.), from which, among other things, the basic articles of faith, principles of management, rights and obligations of members professing a church or religious society must be clear. Pursuant to Article 15 of the above-mentioned Act, the registering authority shall subsequently examine whether or not the establishment and operation of a church or religious society is contrary to this Act and other laws, the protection of public safety and public order, health and morals, human rights and tolerance or whether the rights of other legal persons and citizens are or are not endangered. In

the event that a church or religious society acts in conflict with this Act or the conditions of registration, the registering authority shall carry out the procedure for cancellation of registration. The records of all legal persons that derive their legal personality from churches and religious societies, unless they are subject to other records or registration, are kept by the Church Department of the Ministry of Culture of the Slovak Republic. The register shall include, inter alia - the name of the entity, the address of the registered office, the designation of the statutory body, the registered church or religious society to which the entity belongs and from which it derives its legal personality, date of registration, date of de-registration. However, the list of legal persons deriving their legal personality from churches and / or religious societies does not include the names of specific persons who represent their statutory body. After the amendment to Act No. 308/1991 Coll. of 1 July 2016, the Ministry also registers unexpunged sentences imposed by the court in criminal proceedings, as well as unexecuted sentences affecting their legal successors. The register is publicly accessible.

In 2017, there was a legislative change in the registration of churches (amendment to Act No. 308/1991 Coll.), which in connection with the registration of churches not only adjusted the required number of adult members from the original 20,000 to 50,000, but also specified members as permanent residents in the SR and with Slovak citizenship.

The financing of churches and religious societies was regulated by Act No. 218/1949 Coll. on the economic support of churches and religious societies by the State. Pursuant to the said Act, churches and religious societies are obliged to submit an annual report to the Ministry of Culture of the Slovak Republic on the management of funds provided by the State. Due to the fact that the system of financing churches and religious societies included ideological starting points from 1949, an amendment to the Act was approved with effect from 1 January 2020 (Act No. 370/2017 Coll.). The system of financing churches takes into account the modification of the number of believers of individual churches according to the population census and emphasizes the separate and independent management of churches according to their own budgets. The State will support the activities of churches by providing a contribution or other support (e.g., in the form of special-purpose subsidies or tax relief), which will be only one of the sources of support and financing of church activities, while the sources of financial support will be in particular their own sources of financing, such as contributions from church members, gifts from domestic and foreign natural and legal persons, revenues from own property, revenues from own activities, revenues from public collections, etc., thus achieving a higher degree of independent position and operation of churches in the SR. The Act obliges churches to submit an annual report on the management of the contribution for the previous year, which is public. This ensures transparency in the use of public funds. In order to ensure the correct use of the State contribution by the churches, the State may control the management of the contribution according to special regulations, such as Act of the National Council of the Slovak Republic No. 39/1993 Coll. on the Supreme Audit Office of the Slovak Republic, as amended, or Act No. 357/2015 Coll. on financial control and audit and on the amendment to certain acts as amended.

Statistical overview of the number of churches and religious societies[83]

As of 01.10.2019			number	number of all registered legal persons
Registered churches and religious societies			18	2,905
of which	number of headquarters (bishoprics, dioceses, eparchies...) of registered churches and religious societies			36
	number of basic organisational units (parishes, church congregations, municipalities...) of registered churches and religious societies with legal personality			2,538
	number of other religious legal persons (religious orders, special purpose institutions, associations...)			336
	in it	male religious orders	33	74
		female religious orders	51	81

Register of public collections - registration in the register of public collections can only be made by the local competent authority of the central government, which will receive the proposal for registration of the public collection:

- the district office for public collections to be carried out in the territory of the municipalities belonging to its territorial district,
- the Ministry of Interior for public collections to be carried out in the territory extending beyond the territorial district of the district office,
- the Ministry of Interior with the prior approval of the Ministry of Foreign and European Affairs of the Slovak Republic for all public collections, at least part of the net proceeds of which will be used abroad.

Public collection (Act No. 162/2014 Coll. on public collections and on the amendment to certain acts) may only be carried out by legal persons after the final decision on the registration of the collection in the register of collections. The control of public collections is carried out by the competent administrative authority by means of a preliminary report and a final report. Within 90 days from the date of completion of the collection, the legal person is obliged to submit to the administrative authority a preliminary report of the collection (within the meaning of Article 13(1) of Act No. 162/2014), which shall include:

a) an overview of the execution of the collection,
b) an overview of the gross proceeds of the collection according to the methods of carrying out the collection,
c) bank statements from a special account.

[83] Source: https://www.culture.gov.sk/posobnost-ministerstva/cirkvi-a-nabozenske-spolocnosti/evidencia-cirkevnych-pravnickych-osob/

The legal entity is obliged to submit the final report of the collection to the administrative body within 12 months from the date of closing the collection pursuant to Article 13 (3) of Act No. 162/2014 Coll. which contains:

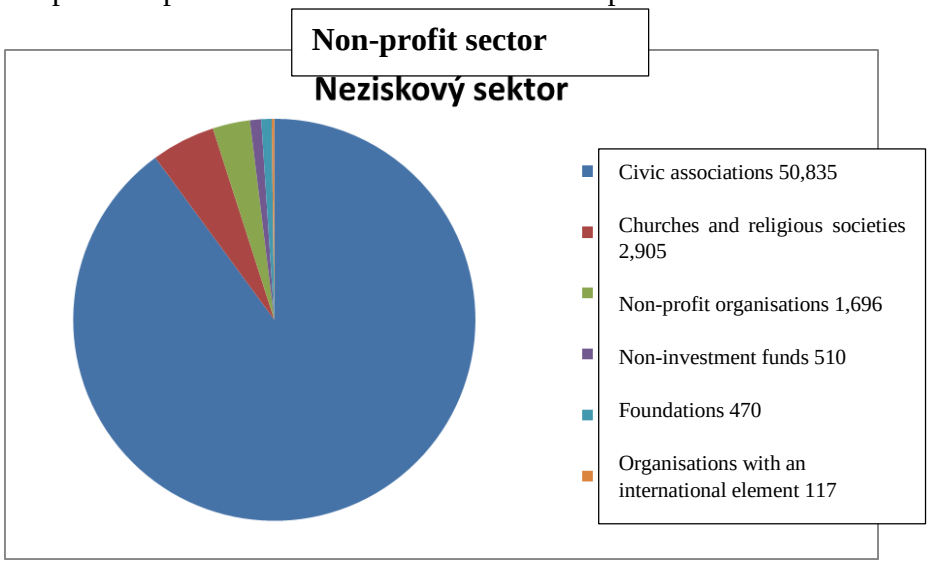
a) collection cost overview,
b) an overview of the use of the net proceeds of the collection for its purpose,
c) documents proving the cost of the collection,
d) documents proving the use of the net proceeds of the collection.

Administrative delinquencies are governed by Article 15 (1) of Act No. 162/2014 Coll., which stipulates the imposition of sanctions in the amount of EUR 100 to EUR 1,000 for breach of the provisions of the Act in question.

Another measure supporting the transparency of the non-profit sector is the provision of information on beneficial owners. The definition of the beneficial owner for pooled asset funds is set out in Article 6a (1) (c) of the AML Act. Pooled asset funds (foundations, non-profit organisations providing welfare services, non-investment funds) are obliged to provide data on beneficial owners when registering from 1 November 2018.

Pooled asset funds that were established by 31 October 2018 were required to provide the registering authority with information on beneficial owners by 31 December 2019. According to the information obtained, only part of the pooled asset funds provided the register authority with information on beneficial owners.

Graphical representation of the size of the non-profit sector as of 31 December 2019:



Control of the non-profit sector in accordance with the AML/CTF Act

The FIU SR is entitled to perform an inspection in the pooled asset fund for the purpose of identifying the beneficial owner and verifying the truthfulness and completeness of data on the beneficial owner, identification of persons or for the purpose of verifying the management of assets. The pooled asset fund has the same control obligations as the obliged entity pursuant

to Article 30 of the AML / CTF Act. The FIU SR may impose fines of up to EUR 200,000 (Article 33 (3) of the AML / CTF Act). In the assessed period, the FIU SR performed 1 inspection in pooled asset funds.

Number of received UT reports in connection with the non-profit sector:

Year	Number of received UT reports (non-profit sector)	Subsequent forwarding of information
2016	10	5 - FD SR; 3 – FIU SR DTB; 2 - LEAs
2017	10	4 - FD SR; 1 - FD SR and National Unit of Financial Police; 3 – FIU SR DTB; 2 - LEAs
2018	3	1 - FD SR; 1 - FIU SR DTB; 1 – Anti-Terrorist Dpt. and SIS
2019	9	3 - FD SR; 2 - FD SR and NAKA PPF; 2 – Criminal Police Dpt. (operational); 1 - LEAs; 1 - FIU SR DTB

An analysis of reports of unusual transactions in relation to the non-profit sector revealed that in none of the cases did they involve suspicions of terrorist financing.

Tax audit in the non-profit sector

The tax authority is entitled to carry out a tax audit for VAT on the non-profit sector, if the entity is a taxable person, on corporate income tax, as long as it achieves income pursuant to Article 12 (2) of Act No. 595/2003 Coll. as amended. It is also possible to perform an accounting check.

Statistical overview of the number of filed tax returns in the assessed period:

Legal form	Number of tax entities filing VAT returns	Number of VAT returns	Number of tax entities filing corporate income tax returns	Number of corporate income tax returns
International organisations and associations	3	68	19	59
Foundation	19	253	323	1,062
Non-investment fund	7	124	178	588
Non-profit organisation	216	5,300	2,594	8,372
Non-profit organisation providing welfare services	5	65	39	71
Organisational unit of association	4	56	549	1,940
Interest association	1	22	54	154
Interest association of natural persons without legal capacity			1	3

Interest association of legal persons	68	2,160	435	1,407
Association (union, society, company, club, etc.)	928	20,865	15,314	46,765
Sum total	1,251	28,913	19,506	60,421

Statistical overview of the number of performed tax audits in the assessed period:

Legal form	Number of VAT audits	Total finding from VAT audits	Number of corporate income tax audits	Total finding from corporate income tax audits
International organisations and associations	-	-	-	-
Foundation	-	-	-	-
Non-investment fund				
Non-profit organisation	15	EUR 274,247.13	2	-
Non-profit organisation providing welfare services	-	-	-	-
Organisational unit of association	-	-	-	-
Interest association	5	EUR 2,932.00	-	-
Interest association of natural persons without legal capacity	-	-	-	-
Interest association of legal persons	-	-	-	-
Association (union, society, company, club, etc.)	42	EUR 107,349.10	5	EUR 36,183.39
Sum total	62	EUR 384,528.23	7	EUR 36,183.39

Statistical overview of the number of sanctions imposed by the tax administrator in the assessed period:

Legal form	Number of sanctions imposed by the tax administrator	Total amount of sanctions imposed by the tax administrator
International organisations and associations	14	EUR 420.00
Foundation	156	EUR 5,088.19
Non-investment fund	23	EUR 1,045.22

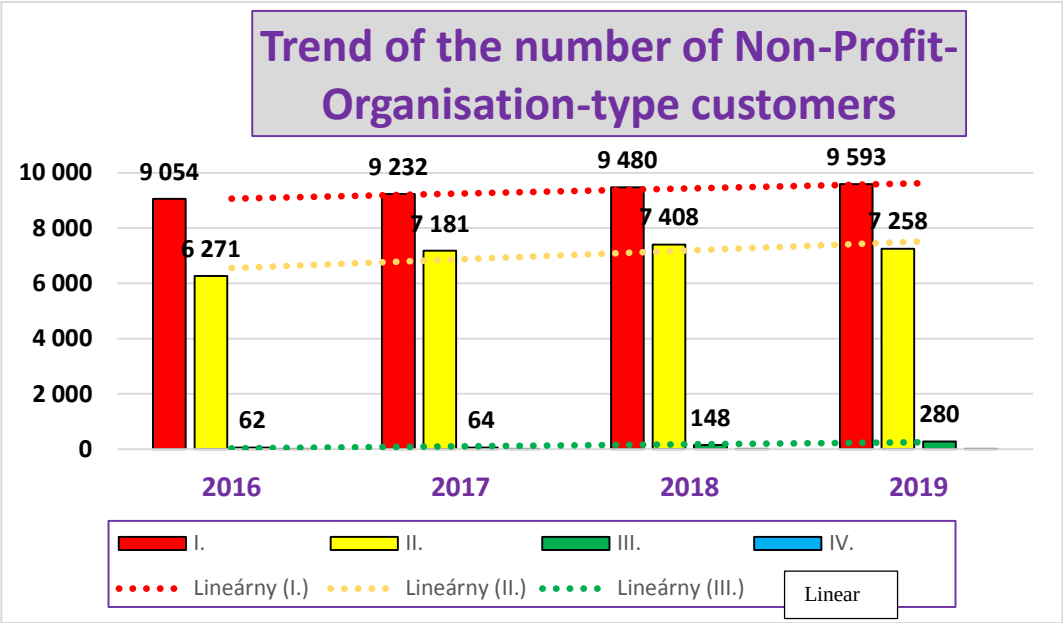
Non-profit organisation	2524	EUR 84,440.91
Non-profit organisation providing welfare services	6	EUR 158.70
Organisational unit of association	103	EUR 14,249.37
Interest association	8	EUR 390.00
Interest association of natural persons without legal capacity		
Interest association of legal persons	322	EUR 19,907.92
Association (union, society, company, club, etc.)	5199	EUR 391,326.83
Total	8355	EUR 517,027.14

Banking sector – non-profit sector analysis

Statistical overview of the number of bank accounts maintained for non-profit organisations:

Number of Non-Profit-Organisation-type customers					
Bank group	2016	2017	2018	2019	2019 /in %/
I.	9,054	9,232	9,480	9,593	56
II.	6,271	7,181	7,408	7,258	42
III.	62	64	148	280	2
Group IV	3	4	5	6	0
total:	15,390	16,481	17,041	17,137	100

Graphical representation of the trend of keeping bank accounts for non-profit organisations:



Based on the evaluation of information and data obtained within the process of the 2nd NRA it can be stated that 29% of banks have special procedures in place for non-profit organisations and 19% of banks provide enhanced customer due diligence to all non-profit organisations. 22% of banks perceive non-profit organisations as high-risk customers and perform enhanced customer due diligence in relation to them, other banks perform basic customer due diligence but with elements of enhanced customer due diligence, especially in detailed determination of the purpose of business relationship, nature of their activities, identification of beneficial owner, sources of financing , monitoring of payments - especially to high-risk countries and also monitoring of their counterparty (recipients of payments). As part of transaction monitoring, banks monitor in particular the geographical aspect. In general, banks perceive non-profit organisations as a riskier segment of customers and, even if they provide them with basic customer due diligence, they perform ongoing monitoring. This approach can be assessed as appropriate in terms of risks - in particular the risks of terrorist financing.

Cooperation between public sector and non-profit sector

In the interest of proper functioning and development of the non-profit sector, the Institute of the Plenipotentiary of the Government of the Slovak Republic for Civil Society Development was established in 2011 and a new advisory body of the Government was established in 2012 - the Government Council for Non-Governmental Non-Profit Organizations consisting of representatives of general government and representatives of non-governmental non-profit organisations. Concepts for the development of civil society in Slovakia are being adopted in cooperation between representatives of the state sector and the third sector, including action plans for the respective years. An important topic of the action plan was the implementation of research in the field of social and economic benefits of the non-profit sector and development trends of civil society in Slovakia, which began in 09/2018 with the expected

completion in 02/2021. The subject of research is the collection, analysis, processing and dissemination of data on the economic and social benefits of the non-profit sector in the context of the current state and development trends of civil society for the purpose of public policy making.

The FIU SR, in close cooperation with the Slovak Government's Plenipotentiary for the Development of Civil Society, conducted a survey on the possible misuse of the non-profit sector for terrorist financing. 22 entities (19 non-profit organisations and 3 civic associations) participated in the survey. Based on the evaluation of information and data, it is generally possible to state that the entities of the non-profit sector perform their activities mostly in the territory of the Slovak Republic and do not provide funds to entities from conflict areas. It can also be stated that the non-profit sector knows its donors well, while donors come mainly from the Slovak Republic. As for the use of funds in cash, only 9% of the addressed subjects accept them. In their activities, 50% of entities do not use cash payments at all and 45.5% rarely use them. No entity has faced, directly or indirectly, the threat of terrorist financing.

The SR has clear legislative rules to support the responsibility, integrity and trust of the public in the administration and management of non-profit organizations, especially through special laws governing various legal forms of the non-profit sector.

Vulnerabilities:

- insufficient supervision of pooled asset funds by the FIU SR – a low number of inspections,
- civic associations within the meaning of the Act on Civic Associations do not have to publish or prepare annual reports, they are not supervised by the register authority (non-transparent environment)
- insufficient education to protect the sector from its misuse for terrorist financing

Vulnerability - low level

Analysis of trends, resources that could potentially be misused for terrorist financing purposes

Intelligence services have identified several potential risk sources and trends that could be misused for terrorist financing.

In the environment of Islamist terrorism, it was possible to observe a trend of decreasing costs for terrorist activities, as the real usable amount of money available to terrorist actors in Europe decreased. On the one hand, this was due to more effective security measures to monitor suspicious financial flows, on the other hand, the response of Islamist radicals to the measures taken in the form of greater caution, as well as change of the modus operandi of terrorist attacks to less costly methods, especially acts of isolated individuals / lone actors, without significant preparation and planning, recruitment, logistics and training.

The funds used to finance terrorist activities may come from the operation of legal companies (part of their profits may go to terrorist financing or serve as cover for the presence

of members of terrorist groups in Europe). Such a case has not been recorded in the Slovak Republic.

Funding for terrorist activities within Europe can also come from criminal activities (theft, robbery, production of false documents, trafficking in drugs and human beings, extortion). The environment of organised crime and terrorism is gradually becoming more and more interconnected. Organised crime is also becoming an important source of funding for Islamist radicals. No case of connection between terrorism and organised crime was recorded in the assessed period in the territory of the SR.

Proliferation

The threat of financing the proliferation of nuclear weapons for terrorist purposes can be assessed as **LOW**, mainly due to the specific approach of countries to controlling the proliferation of weapons of mass destruction (WMD) proliferation (including intelligence services) and in particular nuclear weapons. The threat of financing the proliferation of other types of WMD is also assessed as low, given the complexity of gaining access to WMD and materials used for their production, very high financial costs of their acquisition, technological complexity of their production and handling (storage, transport, etc.). It is likely that the interest of global jihadist groups will focus more on a possible terrorist attack against nuclear power plants or industrial companies and other legal entities involved in the processing and handling of dangerous chemicals (warehouses, ships engaged in the cargo shipping of dangerous goods). However, it is not possible to rule out an attempt to finance proliferation and obtain biological weapons made on the basis of plant extracts (ricin) or mortar shells modified or enriched with chemicals in improvised conditions. For these reasons, funding for WMD proliferation is likely to continue to dominate the activities of world military powers in order to maintain an imaginary balance of their military capabilities, in particular their most effective weapons systems. At the same time, efforts are likely to be made by some states with an authoritarian political regime to acquire WMD. The threat of proliferation of other internationally controlled defence products is assessed as **LOW**. Efforts to obtain defence products will most likely be made through countries that have different foreign policy relations with third countries, insufficient export controls, or the use of corruption by third country officials.

The threat of proliferation of dual-use items in favour of high-risk country regimes, including its financing, can be assessed as **HIGH**. These countries have long been making efforts to acquire sensitive goods, technologies and know-how, and these are tasks assigned directly by the country's management. A sophisticated network of intermediaries is often involved in these activities, with the same inquiries directed to several countries at once.

In an effort to develop WMD (especially the nuclear and missile program), proliferation activities are implemented over a wide range of goods, services and know-how, including the so-called sub-threshold items that do not directly fall under the controlled goods. For these reasons, it is relatively difficult to comprehensively cover the reported area and detect financial flows, which often do not copy the physical flow of the reported proliferative activities.

In the previous period, there were cases of the use of inconsistent Slovak legislation related to expansion weapons to commit a terrorist attack and to trade in them in some EU countries. Until 2015, it was possible to legally purchase weapons through the online store,

which were modified and sold as expansion weapons. However, these weapons could subsequently be reactivated and capable of firing live ammunition after a small technical intervention. For the personal purchase of expansion weapons in the arms shop, it was sufficient until 2015 if a person who reached the age of 18 proved his / her identity. In 2015 and in the following years, Act No. 190/2003 Coll. on firearms and ammunition was amended to eliminate identified shortcomings, including those related to the acquisition of and trade in expansion weapons.

Support measures of the competent authorities of the Slovak Republic in the fight against proliferation / financing of proliferation.

In 2006, the UN Security Council imposed assets freeze restrictions on those it identified as engaging, directly related to Iran's proliferation-sensitive nuclear activities or the development of nuclear weapon delivery systems. Between 2007 and 2012, the European Commission took further action. Iran is subject to financial sanctions imposed by the UN.

In 2013-2017, Iranian banks had difficult cooperation with European banks. Pursuant to Council Regulation concerning restrictive measures against Iran No. 267/2012 (later amended by Council Regulation No. 1263/2012 concerning restrictive measures against Iran) all transactions from EU Member States to Iran and vice versa exceeding the amount of 10,000 EUR required notification. Furthermore, authorisations were required for transfers in excess of EUR 40,000. Council Regulation No. 267/2012 was modified and the amounts were reduced to values for transactions exceeding EUR 100,000 for notification and for transactions over EUR 400,000 for the necessary authorization of the competent authority. Regulation no. 267/2012 also respects the obligations of Member States under the UN Charter and the legally binding nature of UN Security Council resolutions.

In the evaluated period, the Ministry of Finance of the Slovak Republic dealt with 2 cases in the total amount of EUR 157,892.52 in the area of sanctions against Iran - transfers of funds from / to Iran from / to the Slovak Republic were temporarily frozen and later allowed, based on EU Regulation No. 267/2012 later No. 1263/2012 concerning restrictive measures against Iran. In this context, after receiving each case - a request for a transfer of funds, the Ministry of Finance of the Slovak Republic addressed the competent authorities with a call for an opinion on the authorisation of this transfer and the evaluation of the case in question. In the event that all relevant addressed authorities and the Ministry of Finance of the Slovak Republic did not identify such facts that would lead to the fact that the transfer of funds could be in conflict with any of the prohibitions or obligations of the regulation, and at the same time the subject of applications were not dual-use goods, there was no need to continue blocking.

The Slovak Republic is a participating State of the Wassenaar Arrangement “WA”, the Australian Group “AG”, the Nuclear Suppliers Group “NSG” and voluntarily adheres to the principles of the Missile Technology Control Regime “MTCR”. The operation of international dual-use export control regimes, i.e., WA, AG, NSG and MTCR supports and facilitates compliance with the principles and commitments under the Treaty on the Non-Proliferation of Nuclear Weapons “NPT” and the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction.

The control of foreign trade in dual-use goods and technologies is regulated in Act No. 39/2011 Coll. on dual-use items and on the amendment to Act of the National Council of the Slovak Republic No. 145/1995 Coll. on administrative fees, as amended. Act No. 39/2011 Coll. was adopted to bring national legislation in the field of trade in dual-use items into line with EU law (Council Regulation (EC) No. 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items), and to eliminate shortcomings in the applicable legislation governing the area.

Based on Act No. 392/2011 on trade in defence industry products, a Permanent Expert Group was established at the Ministry of Economy of the Slovak Republic for the assessment of applications for an authorisation for the export of defence industry products ("SES"). The members of the group are: Ministry of Foreign and European Affairs of the SR, FACO, SIS, MI, MI SR, Ministry of Economy of the SR, National Security Authority. Within this group, those authorities shall provide each other with sub-opinions for each application for authorisation to trade in defence-related products. The conditions for the operation of the SES are laid down in the "Statute of the Permanent Expert Group".

In the assessed period, the Ministry of Economy of the Slovak Republic conducted 15 administrative proceedings due to the fact that the participants in these proceedings did not fulfil their obligations arising from legal regulations governing permitting and licencing procedures (under the responsibility of the Department of Trade Measures of the Ministry of Economy of the Slovak Republic). The fines were imposed in the total amount of EUR 146,360.00.

Number of cases and financial volume of granted licences for import including transfer to the SR:

Year	Financial volume (EUR)			Number of cases		
	Import (including transfer)			Import (including transfer)		
	Defence-related products	Dual use	Designated products whose possession is limited for safety reasons	Defence-related products	Dual use	Designated products whose possession is limited for safety reasons
2016	167,537,507.06	1,066,500.00	48,952,992.00	555	1	438
2017	275,007,890.63	459,481.00	60,848,074.00	605	6	461
2018	271,148,426.60	6,950.00	57,440,313.00	551	1	442
2019	121,468,274.98	193,285.00	61,074,445.00	576	3	402

Number of cases and financial volume of granted licences for export including transfer to the SR:

Year	Financial volume (EUR)			Number of cases		
	Export (including transfer)			Export (including transfer)		
	Defence-related products	Dual use	Designated products whose possession is limited for safety reasons	Defence-related products	Dual use	Designated products whose possession is limited for safety reasons
2016	207,761,955.80	6,955,700.00	18,534,302.00	389	11	162
2017	228,862,567.20	6,641,880.00	22,675,342.00	400	14	218
2018	188,889,728.64	1,126,289.00	32,719,766.00	375	8	192
2019	149,765,012.60	27,368,559.00	50,501,571.00	314	10	227

Percentage evaluation of countries according to the number of issued licences:

Year	Percentage evaluation of the first five countries according to the number of issued licences - import				Percentage evaluation of the first five countries according to the number of issued licences - export		
		Defence-related products	Dual use	Designated products whose possession is limited for safety reasons	Defence-related products	Dual use	Designated products whose possession is limited for safety reasons
2016	1.	Czech Republic 33%	Russia 100%	Czech Republic 25.5%	Czech Republic 35%	Serbia 36%	Czech Republic 34.5%
	2.	Austria 28%		Germany 25.3%	Poland 14%	Germany 27%	Poland 8.6%
	3.	Russia 8%		Italy 10.7%	Thailand 5%	France 9%	Slovenia 5.5%
	4.	Belarus 6%		USA 8.9%	Bulgaria 5%	Israel 9%	USA 4.3%
	5.	Poland 5%		Austria 6.8%	Austria 3%	Bosnia and Herzegovina 9%	Moldova 3.7%
2017	1.	Czech Republic 43%	Belarus 50%	Czech Republic 26.6%	Czech Republic 44%	Islamic Republic of Iran 21%	Czech Republic 18.5%

	2.	Austria 23%	Russia 33%	Germany 20.3%	Poland 9%	Israel 14%	Poland 10.5%
	3.	Russia 4%	USA 17%	Italy 12.3%	Bulgaria 6%	China 14%	Slovenia 9.2%
	4.	Poland 3%		USA 8.8%	Thailand 3%	Cuba 14%	Austria 6.6%
	5.	USA 3%		Austria 6.2%	Serbia 2%	Belarus 7%	Belgium 3.5%
2018	1.	Austria 29%	Belarus 100%	Czech Republic 24.2%	Czech Republic 49%	Republic of Korea 25%	Czech Republic 22.9%
	2.	Czech Republic 28%		Germany 20.8%	Poland 9%	Russia 12.5%	Poland 7.8%
	3.	Poland 6%		USA 12.2%	Germany 4%	Israel 12.5%	Belgium 5.7%
	4.	USA 4%		Italy 7.4%	Bulgaria 3%	Serbia 12.5%	Germany 3.6%
	5.	Russia 4%		Austria 4.9%	India 3%	Italy 12.5%	Austria 3.1%
2019	1.	Czech Republic 35%	Russia 67%	Czech Republic 27.3%	Czech Republic 39%	China 20%	Czech Republic 24.6%
	2.	Austria 30%	Belarus 33%	Germany 18.9%	Poland 14%	United Kingdom 20%	Poland 8.3%
	3.	Poland 4%		Italy 11.4%	Germany 6%	Vietnam 20%	Hungary 5.7%
	4.	Germany 4%		USA 8.9%	Mexico 4%	Czech Republic 10%	Austria 5.2%
	5.	Serbia 2%		Austria 7.9%	Switzerland 4%	Germany 10%	Slovenia 5.2%

Number of refused applications:

Year	Defence-related products	Designated products whose possession is limited for safety reasons	Dual use
2016	11	0	1
2017	3	3	0
2018	7	6	3
2019	6	6	1

Overview of applications negotiated by the SES:

Year	Defence-related products			Designated products whose possession is limited for safety reasons	Dual use
	Number of applications for authorisation	Number of applications for licences	Total number of applications	Total number of applications	Total number of applications
2016	22	905	927	600	16
2017	21	973	994	682	26
2018	28	865	893	641	12
2019	22	791	813	635	16

- Weaknesses:
- an effective system of proliferation controls is not ensured,
- the procedures of public authorities are not sufficiently coordinated,
- insufficient awareness of the representatives of state authorities in the field of proliferation,
- low level of awareness of dual use know-how proliferation.

Legislation quality

Act No. 300/2005 Coll. Criminal Code

The issue of terrorist financing and terroristic criminal offences is comprehensively regulated in the provisions of Article 419 et seq. of the Criminal Code. It should be emphasized that in 2018 the above provisions were comprehensively amended in connection with, inter alia, Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism, Council of Europe legal norms on combating terrorism, as well as FATF recommendations in this area. With reference to the above legal norms by which the Slovak Republic is bound, separate merits were created with effect from 1 July 2018:

- criminal offence of terrorist attack pursuant to Article 419,
- criminal offence of some forms of participation in terrorism pursuant to Article 419b,
- terrorist financing pursuant to Article 419c,
- criminal offence of travelling for the purposes of terrorism pursuant to Article 419d of the Criminal Code.

Criminal liability of legal persons is regulated in detail by Act No. 91/2016 Coll. on criminal liability of legal persons and on the amendment to certain acts which came into effect on 1 July 2016. This Act also covers possible penalisation of a legal person for the commission of a criminal offence of terrorist attack pursuant to Article 419, some forms of participation in

terrorism pursuant to Article 419b, terrorist financing pursuant to Article 419c, travelling for the purposes of terrorism pursuant to Article 419d.

It is reasonable to assume that such wording takes full account of international standards in the fight against terrorist financing and creates a sufficient legislative precondition for the effective punishment of any form of terrorist financing.

Weaknesses:

- the Council of Europe Committee MONEYVAL identified in the report on the 5th round of evaluation a shortcoming in relation to the requirement to prove intent in Article 419 of the Criminal Code - it is not fully in line with the FATF standard.

Vulnerability - low level

Act No. 297/2008 Coll. on protection against money laundering and terrorist financing

Among the most significant amendments, which aim to clearly streamline the fight against money laundering and terrorist financing, are:

- the act introducing an extension of the term of terrorist financing (financing the daily needs of a person who can be presumed to intend to commit or has committed a criminal offence of terrorism and some forms of participation in terrorism), as well as its very term and extending UT indicators relating to terrorism (Act No. 397/2015 Coll., which, for the purposes of the Criminal Code, establishes a list of substances with anabolic or other hormonal effects and which amends certain acts),
- the act extending the time limit for UT postponement from 48 hours to 120 hours, and after this period the liable person may postpone the UT exclusively on the basis of notification to the FIU SR that the case was handed over to LEAs for additional 72 hours from the original 24 hours (Act No. 444/2015 Coll. amending Act No. 300/2005 Coll., the Criminal Code, as amended, and amending certain acts),
- the act transposing the 4th AML Directive and the acceptance of the recommendations of the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL and the FATF Recommendations, in order to respond effectively to ongoing developments in AML / CFT, in the improvement of customer due diligence conditions (basic, simplified and enhanced), where enhanced customer due diligence also applies to the so-called politically exposed persons; the obligation to identify the beneficial owner already during basic customer due diligence has been enacted and at the same time, the obligation of the persons concerned was introduced to identify the beneficial owner and to keep their up-to-date identification data in paper or electronic form, as well as whether the customer is not a person covered by an international sanction under the Act on the Enforcement of International Sanctions. The limit for the classification of a certain entity as obliged entity in cash transactions was reduced from the original EUR 15,000 to EUR 10,000 and the obligation to perform basic customer due diligence in cash transactions of at least EUR 10,000 and in gambling games of at least EUR 2,000 was set, which promises to make it more difficult to legalise by using high cash

payments. The obligations of pooled asset funds that may be misused for terrorist financing were tightened, and the conditions for the imposition of fines, as well as their amount, for the administrative delinquencies were adjusted to ensure their effectiveness, proportionality and dissuasiveness for the obliged entity (Act No. 52/2018 Coll. amending the AML Act).

Weaknesses:

- the definition of an unusual transaction in the AML / CFT Act is not in line with the requirements of the FATF
- application of enhanced customer due diligence measures to high-risk countries (only applicable to non-EU/EEA countries)

Vulnerability - low level

Act No. 394/2012 Coll. on limitation of cash payments

No amendment to the Act in question was made in the period under assessment. The Act sets the following limits:

- limit for a cash payment not exceeding EUR 15,000.00 if a payment between natural persons – non-entrepreneurs is concerned,
- limit for a cash payment not exceeding EUR 5,000.00 if the transferor or transferee is a legal person or a natural person who carries out a business or other self-employment activity.

Payments that are higher than the statutory limit can only be made as cashless payment.

Weaknesses:

- insufficient awareness of natural and legal persons

Vulnerability - low level

Act No. 199/2004 Coll. Customs Act

In the SR, the obligation to declare cash of a value of EUR 10,000.00 or more or its equivalent is checked on the basis of such obligation provided in Regulation No. 1889/2005 of the European Parliament and of the Council in Article 3. The obligation has been implemented into national legislation in Article 4 of Act No. 199/2004 Coll. According to the above legislation, any natural person entering or leaving the Community and carrying cash of a value of EUR 10,000 or more shall declare that sum on a prescribed form. Regulation 1889/2005 has been cancelled and replaced by new Regulation (EU) 2018/1672 of the European Parliament and of the Council. It improves the system of control of cash entering or leaving the Community. Regulation 2018/1672 expands the system of controls on cash entering or leaving the Union to movements of unaccompanied cash, for example cash entering or leaving the Union in postal packages, courier shipments, unaccompanied luggage or containerised cargo.

Regulation 2018/1672 will be applied from 3 June 2021 but some of its provisions have already been applied since 2 December 2018. The Regulation reflects the international standards to combat money laundering and terrorist financing as prepared by the FATF. The Regulation uses the term “carrier” meaning any natural person entering or leaving the Union carrying cash on their person, in their luggage or in their means of transport. All travellers are obliged to declare such fact orally and then in writing on a prescribed form or immediately in writing mentioning the transported amount to a customs officer of the Financial Administration.

Weaknesses:

- no legislative coverage of transport of cash by freight transportation and postal consignments

Vulnerability - medium-low level

Legal regulation concerning the activity and tasks of intelligence services
Act No. 46/1993 Coll. on SIS

With effect from 1 January 2016, the amendment to Act No. 46/1993 Coll. on the SIS regulates the tasks of the SIS (Article 2 (1) (e) – to obtain, concentrate and evaluate information on terrorism, including information on participation in, financing or support for terrorism, political and religious extremism, violent extremism and harmful sectarian groupings, activities and threats in cyberspace if they threaten state security and illegal international passenger transport and migration. A significant change in the SIS Act (Article 16a) is also the new regulation introducing obligations for legal persons and natural persons who operate a website or provide a domain name. An operation of a website or access to a domain name may be prevented by a court order issued at the request of the SIS if the operation of such website or domain name spreads ideas that support or promote terrorism, political or religious extremism, violent extremism or harmful sectarian groupings. This amendment created one of the most important preventive tools in the fight against the spread of terrorism in cyberspace.

In Act No. 46/1993 Coll., as amended, proliferation, or its financing, is "found" only through Article 2(4) in the form of the implementation of international treaties. That task is set out only in very general terms, while even the international treaties themselves more or less only talk about proliferation and not about its financing. There is no task in this area, for example, unlike the financing of terrorism, which is specified in Article 2(1)(e). The area of proliferation financing cannot be linked to terrorist financing or to terrorism as such (the term proliferation is not a defined term in the legislation of the Slovak Republic).

The issue of organised crime is mentioned in Act No. 46/1993 Coll. in Article 2 (1) (d), which covers all organised criminal activities; therefore, it can be assessed as sufficient in this area.

The SIS cooperates with ministries, other central government bodies and other state authorities in the assessment of materials published for the inter-ministerial comment procedure and the preparation of concept materials. The aim of the cooperation is to draw the submitting body’s

attention to the existence of problems of application practice and to create a legal basis for the proper and required performance of the legal tasks of the SIS.

Act No. 198/1994 Coll. on Military Intelligence

An amendment to Act No. 198/1994 Coll. on Military Intelligence has been in force since 1 January 2016; pursuant to Article 2 (1) (c), the scope of powers of military intelligence is explicitly focused on terrorism including terrorist financing and support, as well as cyberterrorism.

On 1 April 2018, Act No. 69/2018 Coll. on cybersecurity, which comprehensively regulates the area of cybersecurity and information security, came into effect. To ensure cyber defence of Slovakia, Act No. 198/1994 Coll. on Military Intelligence and Act No. 319/2002 Coll. on the defence of the Slovak Republic were subsequently amended. The amendment to Act No. 198/1994 Coll. on Military Intelligence stipulated that Military Intelligence, within the scope of its competence, obtains, concentrates and evaluates information important for ensuring the defence and defence capabilities of the Slovak Republic in Slovakia and abroad, also focused on activities and threats in cyberspace, while being authorized to take appropriate security measures.

Vulnerability - low level

Legal regulation concerning the application of international sanctions

Act No. 289/2016 Coll. – came into effect on 15 November 2016. Amended Act No. 289/2016 (effective from 15 March 2018) regulates the implementation of international sanctions with the aim of securing, maintaining and restoring international peace and security, protecting fundamental human rights, combating terrorism and the proliferation of weapons of mass destruction. It set up the process of enforcing international sanctions in the area of administrative seizure of funds and property of sanctioned persons. It sets out the scope of powers and obligations of the relevant government bodies in the area of administrative seizure of funds and property of sanctioned persons. At the same time, it sets out the process of identifying natural and legal persons threatening international peace, security and fundamental human rights, and the manner of their inclusion and exclusion on / from the list of sanctioned persons. The draft act defines the range of persons responsible for the implementation of international sanctions and the responsible government bodies, as well as their duties and scope of powers. At the same time, it ensures the immediate transfer of UNSC sanctions through the publication of subsequent UNSC resolutions on the website of the relevant government body.

In 2019, the Ministry of Finance of the Slovak Republic issued “Procedures for the effective implementation of the rules for the freezing of financial assets of sanctioned persons in the practice of the SR”.

Weaknesses:

- there is a lack of clear criteria for the inclusion of a person on the list of sanctioned persons as set out in the relevant UNSCR

- there is no formal procedure at national level whereby the SR could request another country to implement an asset freeze
- there is no specific provision in the act in question to ensure the protection of third parties acting in good faith
- in the area of sanctions related to WMD proliferation, the functions of the various State authorities are not clearly defined
- no guidance has been issued to implementing entities not active in the financial market[84]
- Article 13 of the Act on International Sanctions does not clearly refer to the list of guarantees set out in the FATF methodology

Vulnerability - medium-low level

National strategies

In the conditions of the SR, several entities participate in combating terrorism and especially terrorist financing, in particular the Anti-Terrorism Centre of NAKA PPF, FIU SR, SIS, MI, Special Prosecution Office of the SR. The Special Prosecution Office of the General Prosecutor's Office of the Slovak Republic has a special role in this area; its exclusive scope of powers includes all criminal offences of terrorism pursuant to Article 419 et seq. of the Criminal Code, as well as criminal offences committed for a special motive, i.e. acts committed with the intention to commit a criminal offence of terrorism, as well as the criminal offence of establishing, masterminding and supporting a terrorist group pursuant to Article 297 of the Criminal Code, regardless of where in or outside the territory of the SR they were committed. The Special Criminal Court hears all these terrorism offences in the first instance, and the Supreme Court of the Slovak Republic hears any appeals against its decisions. The above-mentioned entities coordinate and cooperate with each other in the fight against terrorism and terrorist financing on an ongoing basis.

The Interdepartmental Expert Coordination Body for Combating Crime – MEKO operates in the SR, which has an indispensable role in ensuring cooperation and coordination of activities, the exchange of information and the setting up of common procedures between all the authorities and institutions involved. It is in charge of 14 groups dealing with various types of crime. Since 2002, these groups have included the National AML/CFT Expert Group NES-LP, which has two subgroups; one of them is a subgroup focused on resolving the issue of terrorist financing and financing of the proliferation of weapons of mass destruction, which was established by a MEKO resolution on 14 February 2017. The financing of terrorism and the financing of the proliferation of weapons of mass destruction poses a significant challenge to the activities of the relevant State authorities and designated entities operating in the public sector, in particular in the area of the provision of financial services. The subgroup was set up due to the need to harmonise and streamline cooperation, exchange of information and stakeholder activities. Given the fact that the crime in question is also a global problem and is not linked to a specific territory or region, it seems necessary to streamline and develop international cooperation.

[84] Procedures for the effective implementation of the rules for the freezing of financial assets of sanctioned persons in the practice of the SR is intended primarily for financial institutions, but can also be used for other bodies

In order to streamline cooperation between security forces, the NATIONAL SECURITY ANALYTICAL CENTRE - NBAC was established on 1 January 2013. NBAC is an analytical, communication and cooperation workplace with nationwide competence for the area of security threats, based on the active participation of decisive state bodies of the Slovak Republic operating in the area of security. The key tasks of NBAC include the preparation of comprehensive analytical assessments of security incidents based on reports received from state authorities of the Slovak Republic, monitoring the security situation not only in the Slovak Republic but also in the world, if these pose a real security threat to the Slovak Republic. Through NBAC, the Slovak Republic is represented on a multilateral platform of **34 partner counter-terrorism centres and counter-terrorism coordinators from Europe, North America and Australia - Cooperation on Terror Threat Analysis Madrid Group (CTTA Madrid Group).**

The Ministry of the Interior of the Slovak Republic prepares a **National Action Plan against Terrorism - NAP** for a period of four years[85], which is a strategic document, and its main tasks include creating an appropriate environment for the subsequent implementation of international obligations, such as bilateral and multilateral agreements, UNSC resolutions, decisions and resolutions of EU institutions or sanctions of international institutions against persons and entities associated with terrorism. The aim of the National Action Plan is to contribute to greater security of Slovak citizens and preparedness of state authorities in the event of a terrorist attack in the territory of the Slovak Republic, against its citizens and interests abroad while strengthening the exchange of information and improving cooperation between the relevant counter-terrorism authorities.

The General Prosecutor's Office of the Slovak Republic and the NES-LP, taking into account the minimal practical experience of the authorities of the Slovak Republic in the investigation and prosecution of terrorist financing offences, in order to verify the effectiveness of the system and to detect limiting processes, in 2017 took a decision to organise an **inter-ministerial exercise** focused on the issue of detection and screening of terrorist financing in the conditions of the Slovak Republic. The exercise took place in February 2018 and was followed by a meeting with representatives of obliged entities (mainly banks, but also insurance companies or other financial institutions). The purpose of this meeting was to communicate directly with representatives of obliged entities, who directly clarified issues, in particular related to the operational procedures for obtaining the relevant information and its scope. In the exercise, participants considered a total of 11 possible terrorist financing scenarios, which aimed to demonstrate the scope of the authorities' powers and the current level of cooperation within and between the relevant authorities. The results of the exercise demonstrated the system's ability to respond to threats, but at the same time identified limiting processes that enabled targeted action to be taken.

After the completion of the 1st NRA, a non-legislation material – the Action Plan to Combat Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction for 2019 to 2022 was prepared and submitted to negotiation of the Government of the Slovak Republic. By its resolution, the Government of the SR approved the

[85] Currently, the NAP is approved for 2019 – 2022

above material and took note of the final report and the Strategic Principles for Combating Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction for 2019 to 2024. The main objective of the AML/TF Action Plan is to eliminate the deficiencies found during the 1st NRA.

Resolution of the Government of the Slovak Republic No. 129/2015 adopted the Concept of Countering Extremism for 2015 - 2019, which is a basic document defining strategic priorities in the area of prevention and elimination of radicalisation, extremism and related anti-social activities threatening fundamental rights and freedoms of persons and the foundations of a democratic state governed by the rule of law.

In the period under assessment, there was also cooperation between the Anti-Terrorism Centre (ATC) of NAKA PPF and the Ministry of Economy of the SR. At the request of the Ministry of Economy of the SR, training was organised in September 2018 focused on specific topics in the area of terrorism, in particular on international terrorist trends, as well as on the area of extremism, focusing on extremist symbolism.

In combating terrorism, the Ministry of Foreign and European Affairs of the SR:

- represents Slovakia in the Council of the EU Working Party on External Aspects of Counter-Terrorism (COTER) and the Council of the EU Working Party on Counter Measures against Terrorism (COMET),
- monitors and evaluates developments in the world situation and measures taken by the international community in the field of counter-terrorism,
- participates in designing, assessing and elaborating concepts for the long-term development of Slovakia's foreign policy in the field of counter-terrorism,
- performs the role of political coordinator in the fight against terrorism in the conditions of the SR towards foreign countries.

Weaknesses:

- the Action Plan to Combat Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction reflects the results of the 1st NRA (2011 – 2015), however, it was adopted only in May 2019 for 2019–2022, which is a considerable time difference.

Vulnerability - low level

Geographic and demographic factors

With its geographic position, area and population (as at 31 December 2019 – 5,457,873 inhabitants[86]), the SR is among smaller countries with a lower influence on the global economy. Like other EU Associated States, it is undergoing major economic changes. Despite the growth of macroeconomic indicators, the Slovak Republic cannot be defined as the financial centre of Central Europe.

[86] Source: Statistical Office of the SR

Migration control and external border security are a major challenge for Europe. The migration crisis and terrorist attacks in several EU countries have highlighted the need to strengthen the EU's external borders and to set up a more effective asylum policy. The Slovak Republic, as a Member State and part of the common Schengen area, is obliged to participate in the implementation of all compensatory measures resulting from the Schengen acquis in force, as a substitute for the abolition of internal border controls. Following this, in 2019 the Slovak Republic adopted the National Strategy for Integrated Border Management 2019-2022.

In 2019, the Slovak Republic participated in the international exercise COOPSEC 2019 together with the partner countries of the Central European Defence Cooperation, and the inter-ministerial interoperability exercise "New Horizon 2019" took place at the national level. EC experts carried out the third evaluation in Slovakia of the level of correct and full application of the Schengen acquis in the area of return, in the area of personal data protection in the visa process and in the area of visa policy.

In the period under assessment, the number of asylum seekers and the number of asylum applications granted in Slovakia were low. In spite of the above, there is a potential threat that the migration crisis will lead to a deterioration of the security situation also in the territory of the Slovak Republic. The greatest concerns are related to the threat of terrorism, the possibility of building terrorist networks on the territory of Schengen and raising funds to finance them.

Vulnerability - medium level

Adequacy of resources

The issue of terrorist financing is one that requires expertise and skilled analysis. The Police Force does not have the required experts in this field, nor the means to finance/train them. In order to train such experts within the Police Force, it would be necessary to allocate funds for their training, technical and software equipment, etc.

Intelligence services have limited capacity in human and financial resources, which they focus on managing their work and tasks in the area of terrorist financing and proliferation.

Given its legal status as the central national unit for the prevention and detection of money laundering and terrorist financing, the FIU SR has not been adequately resourced in terms of staffing and funding in the long term. The resources allocated to the FIU SR are disproportionate to the seriousness and scale of the problem and are fundamentally inadequate to its current needs.

Vulnerability - medium-low level

Effectiveness of the system for reporting unusual transactions related to terrorist financing

During the assessed period, the FIU SR received 283 reports on UTs with suspected terrorist financing. The reports received were subsequently analysed in detail by the FIU SR and, where necessary, assistance was sought from partner foreign financial intelligence units.

Obliged entities are extremely cautious and prudent when sending UT reports in relation to suspected terrorist financing, which can be documented in cases where every single refusal to enter into a business relationship is reported, e.g., not opening an account of an entity from a third high-risk country, or refusing to carry out a transfer of funds to a high-risk country. It can be concluded that obliged persons are diligent in reviewing business operations.

An analysis of the individual UT reports received during the assessment period identified the following trends:

- cash deposits made into the personal accounts of entities from high-risk countries, whereby the account holder requests confirmation of the account balance, then withdraws the funds in cash or transfers them to the personal accounts of other entities from high-risk countries,
- transfers of funds to business accounts from off-shore countries, whereby persons originating in risky countries are the persons disposing of the accounts; the funds are subsequently transferred to other business accounts or withdrawn in cash,
- transfers of funds to the personal accounts of entities from high-risk countries, followed by cash withdrawals.
-

In relevant cases, the results of the analyses are forwarded to the ATC of NAKA PPF[87]. During the follow-up, officers of the ATC NAKA PPF have the possibility to request additional information subject to banking secrecy directly from institutions of the banking sector as well as from other business entities.

The screening of UT reports and the subsequent analysis of the information submitted to the ATC NAKA PPF did not reveal any facts that would confirm the elements of suspicion of terrorist financing.

Number of UTRs received number of pieces of information forwarded to the ATC:

Year	Number of all UTRs received	Pieces of information forwarded to the ATC
2016	3297	93
2017	2636	69
2018	2509	60
2019	2576	61

[87] Until 1 February 2017, Dpt. of Fight against Terrorism of NAKA PPF, then the name was changed to "National Anti-Terrorism Unit of NAKA PPF" and from 1 October 2019 – Anti-Terrorism Centre of NAKA PPF "ATC"

Vulnerability - medium-low level

Effectiveness of the application of the Targeted Financial Sanctions on Terrorism and Terrorist Financing

Pursuant to Act No. 289/2016 on the implementation of international sanctions, if the implementation of an international sanction requires a permit, consent or issuance of another decision - the SIS, the Ministry of Foreign and European Affairs of the Slovak Republic, the MI SR (or also other competent government bodies or other bodies and institutions, if their competence or the subject of their activity is related to the subject of the requested permit) shall provide a statement upon request from the competent government body. Under the AML/CTF Act, the obliged entity is required to detect and report to the FIU SR an unusual transaction "UT". An UT is a legal act or other action that indicates that its execution may lead to the legalisation of proceeds or terrorist financing. It is also, among other things, a transaction:

- where there is a reasonable expectation that the customer or beneficial owner is a person subject to an international sanction pursuant to Act No. 289/2016 (sanctioned person) or a person who may be in relation to that sanctioned person; or
- in which there is a reasonable expectation that the object of the transaction is or is intended to be an item or service that may be related to an item or service that is subject to an international sanction pursuant to Act No. 289/2016.

Obliged entities have the area of protection against terrorist financing included in the Programme of their own activities and fulfil their obligations under the applicable legislation in the area of the application of international sanctions.

During the period under assessment, the FIU SR received 21 UT reports from obliged entities related to suspected international sanctions, which were not, however, **targeted sanctions** in the context of UNSCRs 1267/1999 and 1373/2001, but e.g., "OFAC" economic sanctions, special sanctions of the Ministry of Economy of Ukraine.

In September 2019, the MF SR organised an **"Efficiency Exercise on the issue of freezing the assets of natural and legal persons in the Slovak Republic"**, mainly for the purpose of increasing the efficiency of the application of Act 289/2016 Coll. on the implementation of international sanctions. The decentralization of the competences of the competent authorities within the framework of Act No. 289/2016 results in application misunderstandings or ignorance about the competences and obligations of the competent authorities. These lead to difficult/unresolved private and public sector cases in SR practice. In the framework of the exercise, the competent authorities were informed about their competences and responsibilities in this area. The competent authorities are familiar with the legislative measures, but need to strengthen mutual cooperation and decision-making in this area in order to avoid unnecessary problems, misunderstandings and duplication of work. There is still a shortcoming in this area, namely the absence of a single central coordinating body to cover the complex implementation of sanctioning measures, which would make the system more efficient.

In the period under assessment, the SR did not receive any requests for inclusion on the sanctions list nor did it make any designations under UNSCRs 1267/1999 and 1373/2001.

Deficiencies identified:

- an ambiguous mechanism for placing persons and entities on the sanctions list
- there is no single dedicated authority with a lead role in the implementation of targeted financial sanctions for terrorist financing
- lack of awareness among the responsible authorities of the application of the Regulations in the context of the enforcement of international sanctions

Vulnerability - medium-low level

Efficiency of International Cooperation

Financial Intelligence Unit

International cooperation is regulated by Article 28 of the AML/CFT Act. The international cooperation of the FIU SR is not limited to specific cases of information exchange, but also includes the general exchange of experience, best practices and participation in international working groups and organisations. No international agreements or treaties, and therefore no Memoranda of Understanding, are necessary for the FIU SR to ensure the exchange of intelligence. However, based on requests from some foreign partners, it was and is necessary for various reasons to provide a legal basis for the exchange of information between the individual national financial intelligence units to be able to cooperate with the Slovak FIU. The exchange of information in a global context is governed by national legislation, which is based on the Egmont Group FIU Information Exchange Principles, a platform for the secure exchange of financial information expertise primarily designed to combat money laundering and the financing of terrorism. The FIU SR has been a member of the international Egmont Group since 1997. As a global grouping of national FIUs, the Group currently includes a membership of 155 FIUs. The FIU SR also cooperates with control authorities of foreign FIUs on AML/CTF legislation and application practices.

On the basis of the FIU Director's methodological guidelines, requests are handled on an individual basis, according to the scope of the information requested. Where possible, urgent requests shall be dealt with within 3 working days or immediately and routine requests within 30 working days.

The effectiveness of international cooperation is primarily determined by the extent to which foreign partner FIUs are empowered to obtain and provide the requested information.

Statistical overview of the exchange of information between the FIU SR and foreign countries in the context of the FT:

Year	Number of requests sent abroad	Number of handled requests from abroad
2016	3	6
2017	8	9
2018	4	5
2019	5	3

Deficiencies identified:

- limitations on the exchange of information by partner foreign FIUs (different scope of authorisations)

Vulnerability - low level

SIS and partner services

The SIS is entitled to cooperate with the authorities of other States of a similar focus and scope, as well as with international organisations, in the performance of its tasks. Within the intelligence community, international cooperation in the fight against the financing of terrorism takes place on the basis of multilateral and bilateral exchanges of knowledge, assessments and analyses.

Cooperation with foreign partner services greatly assists in the assessment of terrorist threats. There is room for improvement in international cooperation, particularly in the area of early acquisition and subsequent sharing of information with partners. A large amount of knowledge can only be obtained on an ad-hoc basis after a terrorist attack has been carried out, whether on the identity of the perpetrator or other related information. Another problem is the divergence of national legislation in the possibilities to provide the intelligence obtained to a so-called third party.

MI and partner services

The legal basis for international cooperation between the MI and foreign partner organisations of similar or identical focus is the Act on MI. MI and partner intelligence services, including EU and NATO intelligence agencies, provide each other with mutual intelligence support focused on their respective area of intelligence responsibility and intelligence interest at strategic, operational and tactical levels. Communication channels and conditions are established to ensure flexible mutual information exchange and bilateral expert meetings are organised where necessary.

Vulnerability - low level

Anti-Terrorism Centre of the National Crime Agency of the Presidium of the Police Force (hereinafter the "ATC NAKA")

The ATC NAKA is connected through the PWGT (Police Working Group on Terrorism) channel with counter-terrorism units from 28 countries (EU Member States + Switzerland and Norway), through which there is an immediate operational exchange of information related to the detection, investigation, clarification and documentation of criminal activities in the field of terrorism. The ATC NAKA also uses Europol's communication channel - CT SIENA, which serves to exchange information between counter-terrorism units of EU Member States, third countries and organisations for the purpose of exchanging analytical, strategic and operational information and analyses. It provides direct, secure, flexible, bilateral contact enabling the rapid exchange and verification of information, preferably in urgent cases

that cannot be delayed. The ATC NAKA also exchanged information through legal assistance, seconded police officers, Interpol and Europol. International cooperation within law enforcement authorities was carried out on the basis of precisely defined rules and procedures in order to protect information of a criminal nature.

The Bureau of International Police Cooperation ensures the exchange of information within the framework of international police cooperation in all criminal offences falling within the mandate of the Bureau, including predicate criminal offences. It provides international police cooperation at the request of a domestic or foreign department on a 24/7 basis. The secure Europol application SIENA is preferably used for the exchange of information through the Europol channel.

EUROPOL National Unit: provides information exchange between EU Member States, third countries and organisations for the exchange of analytical, strategic and operational information and analysis. Communication takes place through the SIENA channel.

INTERPOL National Centre Bureau: exchanges information with countries outside the European Union.

National SIRENE Bureau: in the conditions of the Slovak Republic established in January 2004 and incorporated into the organisational structure of the Bureau of International Police Cooperation of the Presidium of the Police Force. It is a special unit for the exchange of supplementary information and personal data on records processed in the Schengen information system.

The area of international police cooperation is at the required level. In isolated cases, there are delays in proceedings depending on the country concerned.

Vulnerability - low level

Judicial cooperation

According to the declarations of the SR to the relevant international treaty, the General Prosecutor's Office of the SR is the central judicial body for the performance of legal assistance at the stage of pre-trial proceedings in its active and passive form. The Ministry of Justice of the SR is the judicial authority at the stage of proceedings before court. In the case of the passive form, if the request of the foreign judicial authority is addressed to the Ministry, the actual execution of legal assistance is delegated to the prosecution authorities. The district prosecutor's office in whose district the requested legal assistance is to be carried out is competent to ensure the execution of the request for legal assistance from the foreign authority. If more than one prosecutor's office is given local jurisdiction, the Ministry of Justice sends the request to the General Prosecutor's Office for a decision on which prosecutor's office will ensure its execution. The prosecutor's office may entrust a police officer with the actual performance of the legal assistance acts. If a foreign authority requests that a court perform an interrogation or other legal assistance act because of the applicability of the act in criminal proceedings in the requesting state, the prosecutor shall submit the foreign authority's request in this part to the district court in whose district the legal assistance act is to be performed for processing. If the

subject of the request is exclusively the act to be performed by the court, the Ministry of Justice shall send the request directly to the competent court (Article 538 et seq. of the Code of Criminal Procedure).

Overview of judicial cooperation concerning terrorism and terrorist financing:

Year	Requests received	Requests sent
2016	-	-
2017	-	1
2018	3	1
2019	4	4

In 2018, the General Prosecutor's Office of the SR ("GPO SR") was requested for legal assistance by the Czech Republic three times. One request for legal assistance was sent in connection with terrorism, where a criminal prosecution was conducted against a citizen of the SR who had been preparing a terrorist attack on the territory of the city of Prague in 2017. Two requests for legal assistance were sent in connection with the terrorist financing and related to one criminal case where persons travelled from the territory of the Czech Republic in 2016 to the territory of Syria, where they were involved in the activities of a terrorist organisation, and where the said persons travelled with the assistance of other persons who provided logistical and financial support, including from collections on the territory of both the Slovak Republic and the Czech Republic.

In 2018, the GPO SR requested the Czech judicial authorities to carry out 1 legal assistance in a terrorist financing case. The content of the requested legal assistance was the performance of acts falling within the scope of a financial investigation - identification of payments sent and received via the Western Union service.

In 2019, the GPO SR handled 4 cases of passive legal assistance (requests from abroad for legal acts, twice from the Czech Republic, once from Austria and once from Germany) in connection with terrorism offences. In the framework of passive legal assistance, the prosecutor's office was not requested for any seizure of property and no arrests were made on the basis of the EAW/ IAW.

In 2019, the Special Prosecution Office of the GPO SR sent requests for legal assistance in terrorism cases in 4 criminal cases (three times to the Czech Republic and once to Turkey), while neither the seizure of property nor the execution of EAW/IAW was requested.

The SR provides the widest possible range of all relevant forms of legal assistance as provided for in the international treaties to which the Slovak Republic is bound in this area. The Slovak Republic considers the processing of legal assistance from some countries to be lengthy and also of insufficient quality and scope.

Vulnerability - low level

TERRORIST FINANCING RISK ASSESSMENT			
		Threat	Vulnerability
Sector of transport of cash		M	M
Sector of payment institutions, payment service agents and electronic money institutions		M	ML
Banking sector		M	ML
Non-profit sector		ML	L
Legislation quality			
	Act No. 300/2005 Criminal Code		L
	Act No. 297/2008 AML/CTF		L
	Act No. 394/2012 on limitation of cash payments		L
	Act No. 199/2004 Customs Act		ML
	Act No. 46/1993 SIS		L
	Act No. 198/1994 MI		L
	Act No. 289/2016 on the implementation of international sanctions		ML
National strategies			L
Geographic and demographic factors			M
Adequacy of resources			ML
Efficiency of unusual transaction reporting system			ML
Efficiency of application of targeted financial sanctions			ML
Effectiveness of international cooperation			
	Financial Intelligence Unit		L
	Intelligence services		L
	ATC NAKA P PF		L
	Judicial cooperation		L

8. BANKING SECTOR

Position of the banking sector in the Slovak Republic

As of 31 December 2019, 27 banking entities were active on the Slovak financial market, including 9 banks, 14 branches of foreign banks, 3 building savings banks and 1 savings and credit cooperative, an organisational unit of a foreign entity. It can thus be concluded that the banking sector is relatively saturated and stable in terms of the number of entities.

The total assets of the above entities amounted to EUR 86,516 million as at 31 December 2019. The year-on-year increase in assets compared to 31 December 2018 amounted to EUR 4,511 million (total assets as at 31 December 2018 amounted to EUR 82,005 million). The banking sector employed a total of 19,393 staff as at 31 December 2019, of which 17,687 were in banks and 1,706 in branches of foreign banks. The banking sector's cumulative profit amounted to EUR 643 million during 2019, which corresponds to a year-on-year growth of only 0.53%.

Banks in the Slovak Republic provide customers with a wide portfolio of products, for natural persons, for the private banking segment of natural persons, for the SME segment, large corporate customers, etc. Some banks provide services exclusively for natural persons or only for the "corporate customer" segment (SME, large corporate customers). Customers of all segments actively use modern technologies enabling remote communication with banks, such as internet banking, banking applications on mobile phones, a wide range of payment and credit cards. A more detailed analysis of processes and products is provided in the following text of the report.

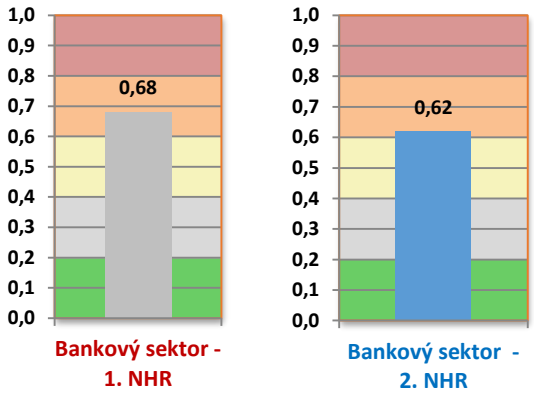
For the purposes of NRA, banks in rounds 1 and 2 were divided into four groups (the criteria for grouping were statistical indicators, in particular: volume of loans granted, volume of customer deposits, number of customers, number of accounts, market share, business model, etc.).

Banks were also asked to provide detailed information, data, documents in the 2nd round of NRA through a questionnaire focused on questions on banking processes, products and statistical data, identified risks. The evidence thus obtained by the working team (from the extensive questionnaire from all banks in the SR) was a valuable source of information for the assessment process of the 2nd round of NRA. Another source of information for the assessment team was the European Commission's report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (the 2019 Supranational ML/TF Risk Assessment Report). The assessment team also took into account conclusions from European Banking Authority (EBA) reports, guidelines and opinions, conclusions from FATF reports and guidelines, as well as its own knowledge and background and experience.

As in the 1st round, the World Bank's assessment tool was also used in the 2nd round of NRA to assess the overall vulnerability of the banking sector. The overall vulnerability of the banking sector in the 2nd round 2 of NRA in the conditions of the SR was determined to be at a

medium-high level based on the assessment of aggregated information and data, with a numerical vulnerability level of **0.62** - see chart (the indicator of the overall vulnerability of the banking sector is lower by six hundredths compared to the value of 0.68 in the 1st round of NRA).

On the one hand, compared to the 1st round of NRA, improvements can be noted in banks' ML/TF risk management practices and processes. On the other hand, it should be noted that the assessment team also analysed new risks in the report, which also had an impact on the riskiness of the sector. The resulting effect of taking these two factors into account is a reduction in the overall level of vulnerability compared to the 1st round, which can be viewed positively. The current value of 0.62 represents the lower end of the interval for a medium-high level of vulnerability, which can also be seen in the graphical comparison of NRA Round 1 and Round 2.



Banking sector – 1st NRA **Banking sector – 2nd NRA**

PROCEDURAL VULNERABILITY OF THE SECTOR:

In terms of assessing the procedural aspects related to the performance of activities and internal processes of individual entities of the banking sector, as well as supervisory and control authorities, it can be stated that a negative impact on the overall level of vulnerability and the most deficiencies were identified in the following areas:

- Efficiency of supervision/control procedures and methods,
- Existence and enforcement of administrative sanctions,
- Effectiveness of monitoring and reporting unusual transactions,
- Existence and enforcement of criminal sanctions,
- Availability of and access to information on beneficial ownership,
- Availability of independent information resources.

The vulnerability of individual processes and their shortcomings can be further characterised as follows:

- Efficiency of supervision/control procedures and methods

In the conditions of the SR dual supervision applies. The FIU SR is primarily entrusted with the supervision of the statutory AML/CFT obligations in the conditions of the SR and supervises both financial and non-financial sector entities. The NBS supervises financial institutions.

The control of AML/CFT compliance obligations is one of the strategic tasks and activities of these authorities. Supervision and control do not only include "on-site" or "remote" supervision, but also support for raising AML/CFT awareness of entities through training, coaching, issuing guidelines, etc. A negative phenomenon affecting not only the actual performance of control/supervision but also the above-mentioned training activities in the period under assessment was the understaffing of the FIU SR and NBS staff responsible for this area. The assessment also found a negative impact in relation to the scheduling and frequency of inspections and surveillance. The NBS takes a risk-based approach to supervision, has its own methodology based on entity risk assessments, but should develop a process to determine how entity-specific ML/TF risk assessments impact on the frequency, scope of future on-site/remote supervision. The FIU SR does not conduct remote monitoring of entities. When conducting on-site inspections, it does not have a set process for determining frequency, scope of inspection based on entity-specific ML/TF risk assessment.

There is also room for improving cooperation between the two supervisory authorities in the communication of the conclusions of inspections, supervision.

- Existence and enforcement of administrative sanctions

It can be stated that inconsistent approach of the FIU SR and the NBS persists (e.g., different opinion, view, approach of the FIU SR and the NBS to the identified deficiencies in supervision/control, which subsequently negatively affects the activity of banks by creating ambiguity and uncertainty in the procedures). The range of sanctions imposed so far by both authorities cannot be considered sufficient. The FIU SR did not complete any inspections in the banking sector during the period under assessment. The NBS carried out 34 on-site supervisions in the banking sector during the period under assessment. It tends to prioritise corrective measures in its supervision and less frequently imposes fines in the lower bands. In addition, the FIU SR does not have the statutory power to sanction a natural person - for example, a statutory officer or other responsible employee of an entity. The need for increased cooperation between the NBS and the FIU SR was also highlighted by Moneyval's experts in their evaluation report for the SR in the chapter on supervision.

- Effectiveness of monitoring and reporting unusual transactions

Monitoring and subsequent reporting of UTs is the basis for the effective functioning of the AML/CFT system in the SR. It can be noted that banks have adapted (and are continuously adapting) their information systems to the scope of products and services provided, taking into account the level of their riskiness. The analysis of the responses from the banks' questionnaires shows that all banks have made progress in the quality of the systems for reporting UTs compared to the first round of NRA, such as: automated application for reporting UTs, automatic notification to a designated person in case of a change in the customer's risk category, etc. In 12 banks and branches, there have been staff increases in the AML/compliance units

ranging from one to three new employees. The extent and structure of the updates made to AML procedures during the period under assessment can be assessed positively and this creates a prerequisite for process improvement.

However, a major and persistent negative impact in this area is the insufficient application of customer due diligence measures - basic customer due diligence measures and enhanced customer due diligence measures. The shortcomings are particularly evident in the verification of the origin of customers' funds in ascertaining the purpose and nature of the transaction or business relationship. Banks do not sufficiently assess the level of riskiness of their customers, resulting in a disproportionate ratio between "standard" and "increased" risk customers. On the other hand, however, it should be noted that the number of enhanced customer due diligence and PEP customers has increased (albeit marginally) compared to the first round of NRA, which creates a presumption of improvement in the approach to risky customers *(Note: further information on the number of UTs received by the FIU SR, the customer structure at EDD and CDD, the number of PEP customers, the number of natural-person and legal-person customers is provided in the Annex Tables and Charts: P1 to P5 at the end of the report).*

- Availability of and access to information on beneficial ownership

Compared to the previous NRA, it can be noted that there has been an improvement in this area. The SR has a register in place which is maintained by the Statistical Office. Banks have access to the register. On the negative side, the Register of Beneficial Owners is not 100 % completed and the Register of Public Sector Partners has not been migrated to it. Banks therefore have to continue to rely on manual processing and retrieval of information on beneficial owners and continue to point to the risks associated with the difficulty of accessing information on beneficial owners and the difficulty of identifying beneficial owners in the case of opaque corporate customer structures. In relation to the risks of difficulties in accessing information on beneficial owners, banks have added new questions to the KYC questionnaires or will only allow a relationship with a customer (who has a complex ownership structure) in the form of a face-to-face visit to a trading venue. The banks' activities in this respect can be assessed positively. Overall, however, the situation regarding access to information on beneficial ownership is not satisfactory.

- Availability of independent information resources

Despite some improvement, which is also related to the previous bullet point, banks make insufficient use of these sources to obtain additional information. Furthermore, there is a lack of exchange of information within the limits of the legislation between the different entities of the banking sector, in particular the exchange of negative information on banks' risky customers and information related to fraudulent activities of customers.

General information on the conclusions from the 1st round of NRA
Implementation of NRA conclusions into banks' practice

Banks have actively dealt with the conclusions of the 1st round of NRA. They have improved the efficiency of processes, updated staff training, and increased the quality of monitoring systems.

In addition to process improvements, they also addressed the three riskiest products from the 1st round of NRA: SME payment account, payment account for large legal persons, private banking, and took several ML/TF risk mitigation measures.

The measures for SME payment accounts and payment accounts for large legal persons were mainly related to the tightening of the conditions for the "entry" of customers into the bank (tightening of the procedures for exercising customer due diligence, modification of the KYC questionnaires, clarification of the questions in the questionnaires).

Other measures related to the approval of these customers by the AML Unit or the Special Committee, as the case may be. Banks were also more rigorous in monitoring transactions. Measures relating to private banking related in particular to the tightening of the verification of the origin of customers' assets and funds.

The arrangements for the above risk products can be seen as adequate (with caveats in the areas of CDD and EDD).

Framework information on banks' activities in the assessment period of the 2nd round of NRA (2016-2019)

Identification of new ML/TF risks and the measures taken

During the period under assessment, banks identified a number of new risks, such as: i.) risks related to the obligation to make payment systems available to new payment service providers under the provisions of the new PSD2 Directive (these are generally FinTech companies), banks found that these companies do not have adequate AML/CFT control mechanisms and are not subject to supervision, ii.) risks related to customer identity theft, iii.) risks related to the area of innovative technologies (cryptocurrencies, crypto-assets, crowdfunding), iv.) risks of internal nature, related to weaknesses in processes.

Banks have taken mitigating measures to address the above risks, such as: i.) for risks related to access to payment systems by third parties (FinTech companies), banks have applied enhanced due diligence, even in cases where these companies are licenced by an EU regulator, ii.) for identity theft risks, they have introduced fraud detection training for employees, iii.) as part of the measures, they also regularly alert customers through their website or internet banking to possible types of fraud, iv.) for other emerging risks, they have taken appropriate measures, such as improving the customer relationship approval process, adopting a dual approval procedure, etc.

Updates of AML IT systems

During the assessment period, all banks made changes of a major (implementation of new systems) or minor (updates to existing procedures, processes) nature that ensured improvement, acceleration, streamlining of AML systems and processes.

The number of banks with manual systems has decreased compared to the 1st round of NRA. Five banks started using an automated system during the period under assessment. Two banks improved features in the manual system. Further improvements in the manual systems were made by banks in the area of updating sanction lists and PEP lists.

This can be seen as a positive development. There is a presumption that it will bring a higher level of efficiency to the work of the AML units. The activities of banks and branches in their efforts to update processes and procedures can be assessed positively.

Updates of AML processes

In addition to changes in IT systems, banks have also made changes in AML procedures and processes, such as: i.) introduction of new AML/compliance committees to assess new customers, ii.) online supervision of AML department in providing care to non-residents, iii.) introduction of anti-corruption procedure in AML procedures, iv.) tightening of procedures for KYC rule (more detailed policies and procedures), v.) establishment of a KYC team to approve on-boarding of new customers and collaborate in the ongoing monitoring and review of existing customers, vi.) tightening of procedures for pre-employment screening of employees (to check the employee's propensity to be complicit in potential criminal activities), vii.) a mechanism for regular meetings between the AML/compliance unit and the Bank's sales and product departments to monitor current AML/CFT issues (consultation on NBS supervision results, etc.).

The training of bank staff should be considered an important area. Banks have made significant progress in this area, as an example: i.) setting a limit on retesting (identified deficiency from the 1st round of NRA), ii.) AML department will train each branch with emphasis on practical cases of UTs, examples on tracing the origin of customer funds iii.) introduction of a system of so-called “compliance ambassadors” (customer employees of branches in senior position are also "extended hands" for the AML department - the above mentioned system has increased the frequency of familiarization of employees with planned and implemented AML innovations and measures), iv.) increased emphasis on the private banking area (tracing the origin of customers’ money and continuous monitoring), v.) introduction of e-learning as a standard form of training with subsequent testing of knowledge, vi.) tightening of testing conditions with the prevention of sharing of "cooperation" of employees during testing, etc.

Banks have added more practice, ML/TF typologies to training, which creates a prerequisite for better understanding of AML issues by employees (e.g., specific training on ML/TF typologies, AML schemes, on identification of beneficial owners, on verification of customer identification).

As an example suitable as a “best practice” for other banks: training focused on process knowledge throughout the “life cycle” of the customer relationship, which can enhance the quality of ongoing monitoring and the overall customer relationship. Another good example is the “compliance ambassadors” project mentioned earlier in this section.

ML/TF risk management according to risk factors

Directive (EU) 2015/849 puts the risk-based approach at the heart of the fight against money laundering and terrorist financing. ML/TF risk can vary and a risk-based approach helps to manage this risk effectively. Financial institutions need to identify and understand the details of their customers as a focal point of the risk-based approach in the process.

In the Slovak Republic, in accordance with the provision of Article 20a of Act No. 297/2008 Coll., the obliged entity is obliged to identify, assess, evaluate and update the ML/TF risks taking into account the risk factors in the framework of the activities under this Act. Therefore, the assessment team also addressed the management of ML/TF risks according to risk factors in the analysis.

Risk analysis according to product types

Banks have adequate mechanisms in place to manage ML/TF risks associated with products. They use sophisticated IT tools and models to manage risks. In risk management, they generally use product segmentation by the very nature of the product (whether the product allows unlimited transactions, deposits, cash withdrawals, cross-border transactions, etc.).

Risk analysis according to customer types

Also, for the customer risk factor, banks use IT tools to determine the overall riskiness of customers. In the risk management process related to the type of customers/beneficial owners, banks consider risks related mainly to the business or professional activity of the customer/beneficial owner, the reputation of the customer/beneficial owner, the nature and behaviour of the customer/beneficial owner. They also consider customer country risk, the presence of the customer at the opening of the contractual relationship, PEP risk, sanctions lists, the number of UTs connected with the customer.

Risk analysis according to geographic aspects

They take a similar approach to managing risks by geography as they do for product and customer risk factors. They respect EU and FATF legislation, in particular in terms of identifying countries that do not have the same or comparable level of AML/CFT measures as EU countries, as well as identifying countries with strategic deficiencies. In addition, they also use their own lists of high-risk countries.

Risk analysis according to the distribution channel

Where remote customer identification technologies are used, banks will assign a higher risk to the customers so acquired. At the same time, they use measures to mitigate this type of risk (they provide this type of identification only to residents and persons over 18 years of age and only for selected types of products). In the case of acquiring a customer through the bank's intermediary, they conclude a business relationship with the customer when signing the contract in person at the bank.

In managing risks according to risk factors, banks use sophisticated procedures that can be described as appropriate to the risks to which they are exposed in their business.

Managing risks related to cash operations

Deposits and withdrawals to/from the account

Banks that allow cash deposits into and withdrawals from accounts manage the risks associated with cash transactions using set scenarios. For cash transactions, bank staff are required to identify the person of the depositor and his/her relationship to the account holder, ascertain the origin of the funds depending on the ML/TF risk, the purpose of the transaction, the ownership of the funds irrespective of the amount of the transaction, and acting on their own behalf by written declaration, etc. Cash transactions pose a risk of interruption of financial flow monitoring and continuity, as well as a risk of placing illegal money in the legal financial system.

All banks that provide cash services uniformly stated that they monitored and reviewed one-off/irregular cash deposits (they have an alert system based on pre-set scenarios). Banks also monitor, verify high frequency cash deposits/withdrawals (this process is either fully automated or manual in combination with automation and communication with branches, which contact the customer if necessary to provide information and documents proving their origin and purpose).

Banks monitor cash-related risks in detail and have them embedded in their AML Programmes. Examples of identified risks include: i.) cash deposit risk for companies with a business model based on higher cash frequency, currency exchange offices, pawn shops, casinos and gambling houses, used car dealers, secondary raw material buying, construction (especially cash payouts), ii.) higher deposits and withdrawals made on the accounts of natural persons that do not have an economic purpose and for which the customer indicates the reason for the transaction as "savings, partner's contribution to the business, sale of real estate settled in cash", etc., iii.) deposits of third parties into accounts (especially persons who are not entitled to dispose of the account), iv.) excessive and frequent withdrawals from ATMs, v.) lack of enforcement of the obligations arising for legal persons and natural persons from the Act on limitation of cash payments (Act No. 394/2012 Coll.), vi.) customers do not know (do not want to) indicate the origin of money, associated with, e.g., payment of instalments, vii.) early repayment of loans in volumes that are not in line with the income declared in the loan application and in the income certificate, viii.) risks related to the use of credit cards when the turnover on the card account is not in line with the customer's income, ix.) risks related to unreported cash withdrawals in high volumes that were made immediately after the money was credited to the account, etc.

Among the negative facts that adversely affected the vulnerability of the banking sector in both the 1st and 2nd rounds of NRA were the risks associated with cash and the enforceability of Act No. 394/2012 Coll. on limitation of cash payments (the Act contains a number of exemptions, e.g., the prohibition to make certain payments in cash does not apply to payments handed over to or received in the course of the provision of payment services in banks).

The analysis of the trend in deposits/withdrawals in/from accounts *(see Annex Tables and Charts: P6 and P7)* shows that cash associated with accounts contributes significantly to the ML/TF vulnerability of all such customer products. A shortcoming and negative

phenomenon identified during the 1st and 2nd rounds of NRA is the lack of application of basic and enhanced due diligence measures: i.) verification of the origin of customer funds for ML/TF risk, ii.) ascertaining the purpose and nature of the trade or business relationship. Thus, the above-mentioned deficiencies may result in a reduced quality of recognition and reporting of unusual activity, which may lead to a reduction in the effectiveness of the FIU SR and the LEAs.

Deposits through ATMs

Approximately 40% of banks have a network of ATMs in connection with which they monitor their customers' cash withdrawals. Approximately 20% of banks also use ATMs with a deposit function. To mitigate the risks associated with ATM deposits, banks have taken measures such as: i.) analysing the potential risks, in particular with regard to the type of customer, ii.) taking into account the customer's line of business where cash deposits of revenues from the customer's business establishments are common and have an obvious economic purpose, iii.) introducing a limit on cash deposits through ATMs, iv.) increasing the limit on cash deposits through ATMs is approved by the AML/Compliance Dpt., v.) a customer can make cash deposits through ATM only on their own account, vi.) deposits through ATMs are monitored by the AML department and in case of any abnormality/suspicion, customers have to declare the origin of funds. **It may be noted that the banks using ATMs with a deposit function are carefully analysing the risks associated with deposits and we consider the practices of the banks to be reasonable.**

Managing the risks related to politically exposed persons (PEPs)

It may be noted that banks are cautious in their approach towards PEP customers. Most banks (about 80%) use external databases to check PEPs. All banks have mechanisms in place to identify whether a customer is a PEP. A combination of declaration and checking of the customer in public databases/registers is prevalent in the procedures. Banks have also set up a PEP verification mechanism which is directly linked to the PEP identification process. Once identified, the PEP is verified against publicly available sources in order to obtain as much information as possible to process their profile, activities, etc. All PEP customers (new and existing) are regularly checked against existing lists. Banks provide PEPs with enhanced due diligence and strictly verify the origin of assets and money used in PEP transactions. The verification mechanism for PEPs can be considered appropriate to the risks in relation to PEPs. The model of exercising due diligence can be outlined in the following forms: i.) enhanced due diligence, ii.) closing of the trade generally in the physical presence of the PEP at the bank, iii.) approval of the business relationship by the AML/Compliance department, iv.) enhanced ongoing monitoring, v.) tracing of the origin of money and assets. **Banks take a conservative and prudent approach in relation to PEPs and manage ML/TF risks appropriately for this category of customers** *(For further information on the number of PEP customers, see Annex Tables and Charts: P3).*

Managing the risks related to private banking services (PB)

PB services can be seen as providing a highly superior service to solvent and important customers with a range of products and advice that are tailored to individual customer

requirements. PB was provided by seven banks during the period under review. Four of these banks assessed the risk of PB customers as high and automatically provide enhanced due diligence to all PB customers. The remaining banks take a risk-assessed, individual approach to the provision of due diligence, with a predominance of enhanced due diligence customers. Compared to regular retail customers, they treat PB customers differentially: i.) they do significantly more screening of customers they place in the PB segment, ii.) the acceptance of a new customer is longer, iii.) more levels of management approve it, iv.) for a PB customer, the bank considers significantly more documents and information, v.) they focus mainly on verifying the origin of assets and funds. For PB customers, they also carry out more detailed monitoring during the course of the business relationship. However, the fundamental difference is in the frequency and extent of ongoing monitoring of PB customers compared to regular retail customers.

Banks that have customers classified at elevated risk require the following framework of information and documents: i.) documents proving the origin of assets and funds, ii.) the customer's account statement from the bank from which they transfer their money (so that the bank providing PB services knows the genesis of the cash flow), iii.) documents proving assets (e.g. inheritance proceedings, proof of winnings, income from employment, from business), but also iv.) documents on the ownership structure in terms of beneficial ownership, v.) proof of lease, etc. It may be noted that banks have set up processes for effective customer relationship management in the PB segment, which is generally considered risky in terms of ML/TF.

However, the area of reporting of UTs of PB customers can be considered a vulnerability. There is very limited reporting of UTs by banks to the FIU SR for PB customers (UTs are generally sent only after the customer has been publicised in the media). The FIU SR received a total of 115 UTRs from banks for PB customers in the period 2016-2019. In the period of the 1st round of NRA, very few UTs were reported by banks in relation to PB customers, so the above 115 UTRs can be seen as positive, but at the same time there is also considerable variation in the number of UTs reported by individual banks (ranging from 1 to 45 UTs). However, this is still a relatively low number of 115 UTs reported per PB customer relative to the total number of 8,587 UTs reported for all customers from banks that provided the PB service, which represents a 1.34% share). From the above, one can make an assumption of a different approach of banks in assessing the riskiness of PB customers and their business operations. The most common reasons for UTR for PB customers clearly included: i.) high cash deposits in a personal account (cash transactions were reported by all banks), ii.) non-cash transfers in high volumes (e.g., declared as loans) - these were generally transactions that did not match the volume and structure of the information the bank had obtained about the customer, iii.) high non-cash transfers to a personal account from abroad, etc. From the prevalence of cash transactions, it can be concluded that the risk related to cash is still high in the PB segment as well. In this context, a related risk should also be noted - that the act on limits on cash transactions is not observed in practice and, in conjunction with the high volumes of transactions, both cash and non-cash, their excessive use in the PB segment appears to be a particularly high ML/TF risk. In this context, it is the reporting obligation of banks in the PB segment (seven banks reported only 115 UTs over the four-year period under assessment), in proportion to the 20,782 PB customers, the vast majority of which are classified in the high-risk category, that can be seen as a vulnerability.

In the future, supervisory and control authorities will need to pay more attention to this issue and also focus on the education of entities.

Managing other risks

Monitoring dormant accounts

Dormant accounts pose a risk to ML/TF, in particular in the context that, despite a prolonged period when no movements are recorded in the accounts, these accounts remain fully operational and can be activated by customers at any time - for example, by executing a cash or non-cash transaction. Therefore, the assessment team analysed the risks for these types of accounts. Banks prudently monitor and review dormant accounts. The framework mechanism can be described as a combination of running scenarios followed by the generation of an alert after a pre-set time period or after a movement in the dormant account. They have also set up a process for monitoring significant changes in the customer profile. They will record the changes as part of ex post monitoring or in accordance with KYC rules and also during periodic review as part of the risk category reassessment. **It can be concluded that the banks' processes include an internal system whereby ongoing changes in customer profiles have an impact on the execution of follow-up by the banks' staff.**

Regular review of AML due diligence

Banks have procedures in place for periodic review of due diligence. Most banks have the following intervals for reviewing customer due diligence: low risk - 1x/5 years, medium risk - 1x/3 years, high risk - 1x/year. Review systems are generally related to customer size, customer structure, bank structure and business model. In addition to the review of customer due diligence, banks also regularly update the management systems for the exercise of due diligence as part of their AML programmes. **It can be concluded that banks have adequate systems in place to regularly reassess due diligence.**

Managing the risks related to safe deposit boxes (SDB)

Risks in relation to the SDB service were briefly described in the 1st round of NRA, with the vast majority of these risks also noted in the 2nd round (the assessment team ascertained numbers of customers, numbers of SDBs and also focused on UT reporting in relation to the product). Although the principle of discretion is declared by banks in handling the content of a SDB by a customer, paradoxically it is this principle that contributes significantly to the riskiness of the product.

The SDB service is provided by eight banks. The largest banks in Group I have the largest SDB network in their branches. The number of SDBs within each bank ranges from 180 boxes to 3,435 boxes. Banks do not rent SDBs from other external entities; they operate only their own SDBs. As at the end of 2019, banks rented 16,348 SDBs, for 9,610 customers (some customers probably used multiple boxes).

As regards the recording of customers entering the SDBs, all banks confirmed that they only monitor the entry of customers/depositors, record the date, time, identify the

customer/depositor accessing the SDB, and subsequently record the entry in the manual records or in the banking system. The analysis of the responses shows that banks apply different forms of customer due diligence with SDBs and have a different approach to the risks associated with their use (however, they are fully aware of the risks associated with BS). Five banks indicated that they provide basic due diligence to customers. One bank automatically exercises enhanced due diligence in relation to customers with SDBs. Two banks indicated that they exercise the extent of due diligence depending on the risk of the customer, the type of customer, the geography, the structure of the customer (if it is a legal person) and also depending on whether the customer already has other products in addition to SDB in the bank. Approximately 70 % to 95 % of customers use another product in addition to the SDB at the bank (most commonly: current account, savings accounts, fixed-term deposits, exceptionally a combination of SDB and credit, mortgage, etc.).

The following risks can be mentioned in relation to SDBs: i.) the bank cannot ascertain the contents of the box under standard conditions (without an order from the police, court, notary, etc.), ii.) it is a limited area for ascertaining information about the purpose and nature of the business relationship, iii.) the existing ML/TF risk mainly due to the possibility of depositing large amounts of cash or other assets with unclear or non-transparent origin, iv.) cash/other assets with unclear origin can be deposited by one person (owner) and withdrawn by another person (a person entitled to dispose of the box), which may not be a family member of the SDB owner, but may be a stranger.

In relation to SDB risks, the assessment team also took into account the conclusions of the 2019 EU Supranational Risk Assessment Report. In the section for SDBs (Chapter 18 of the report), it is noted that the ML threat and vulnerability level for SDBs is significant (level 3 on a 4-level scale), in particular due to the possibility of hiding proceeds of illegal crime in SDBs (in particular, avoiding tax audits, threat of tax evasion, etc.).

A combination where the owner of the SDB is also a PEP can be considered a high ML risk, in particular due to the possibility of storing large amounts of cash or other high value, low volume assets (precious metals, stones, etc.) that may have illegal or non-transparent origin related to the PEP's activities. **The low number of reported UTs related to SDBs can be considered a vulnerability (the analysis shows that only one bank reported an UT for a PEP). The number of 13 reported UTs in four years out of a total of 16,348 functional SDB and in the context of the risks mentioned above can be considered very low. Banks should look more closely at the process of due diligence, and, in particular, if the customer does not use other products of the bank, they should find out as much information as possible about the purpose and nature of the business relationship with the customer (assumption of frequency of visits, relationship between the owner and the person authorised to dispose of the SDB, finding out the reason for the use of the box, etc.).**

As a best practice for other banks, we can recommend: monitoring of all customer visit documents to the SDB at regular intervals (e.g. the AML department can subsequently check SDB visitors in internal and publicly available databases, with a focus on detecting negative information from the media about their possible criminal prosecution, etc.). A bank applying this procedure also evaluates the frequency of visits to the SDB and, if it assesses it as suspicious, proceeds according to the AML Programme.

Entering into business relationships without the customer's physical presence

Entering into business relationships without the customer's physical presence at the bank and without using technology to reliably identify the customer remotely may pose a higher risk. The analysis shows that about 20% of banks conclude business relationships with customers on the basis of remote identification technology, which uses, for example, facial biometrics or video calling. When using these procedures, banks have taken measures to mitigate risks such as: they use remote identification technologies only for products such as current account or limited consumer credit, for residents over 18 years of age with permanent residence in the Slovak Republic, not for PEPs, not for risky customers on the internal list (black-list), they cooperate with the Ministry of Interior of the Slovak Republic in verifying the ID documents of the potential customer.

The vast majority of banks that use digital "on-boarding", or other forms of remote dealing, execute enhanced customer due diligence in relation to these customers and monitor the customer closely at the initial stage of the relationship.

Approximately 40% of the banks stated that they exceptionally use a courier or accept the concept of a power of attorney with an attestation of signature by a notary public (some banks also approve these authorisations at the AML department). Around 40% of the banks establish relationships with customers only when they are present at the bank. Where a business relationship established remotely has been terminated, banks did not give ML/TF-related reasons for terminating the customer relationship. One bank reported that in a few cases, customers acquired remotely had carried out small-scale internet frauds for which the bank terminated the relationship with them, while redesigning processes and eliminating these risks. **It can be noted that digital technologies for identification and verification of identification were not widespread during the assessment period and banks had adequate risk mitigation measures in place** *(Note: further information on the number of customers with whom a business relationship was established without their physical presence in the bank branch - P9).*

Crowdfunding

Crowdfunding can be considered an open call to the public to raise funds for a specific project. Crowdfunding platforms are generally websites that allow interaction between financial collections and individuals who are interested in contributing financially to a project, possibly for the purpose of increasing the value of their funds.

Banks did not identify customers in their portfolio who intermediate or provide services related to crowdfunding. However, they indicated that they had identified risks related to crowdfunding and some had incorporated them into their AML Programme, although they do not provide the service. Banks consider crowdfunding as a risk factor in terms of ML/TF and payments that have signs of crowdfunding are assessed as high risk by the transaction monitoring tool. Some banks indicated that they did not provide crowdfunding services, referring to group-wide strategies. No bank reported a crowdfunding-related UT during the assessment period.

The risk analysis also took into account the conclusions of the 2019 EU Supranational ML/TF Risk Assessment (Chapter 6). The analysis of crowdfunding vulnerability for ML purposes shows a "medium significant" degree (2/4).

Given the potentially higher risks in some of the schemes of this way of project financing (non-transparency, illegality, crowdfunding service providers either not at all or insufficiently identifying the participants of their scheme), it would be advisable for banks to monitor transactions that have crowdfunding characteristics precisely in the framework of transaction monitoring - even in a situation where they have no official knowledge that the customer is implementing the service. This area is seen by the assessment team as a vulnerability.

Virtual assets (VA)

The FATF definition of VA: "A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes, which does not include a digital representation of fiat currencies, securities and other financial assets". VA is a term broader than virtual currencies.

The analysis also took into account the findings of the 2019 Supranational Risk Assessment (Chapter No. 12). The ML analysis shows that law enforcement authorities have information that suggests that terrorist groups may use virtual currencies or assets to finance terrorist activities. Therefore, the terrorist financing threat associated with virtual currencies is considered significant (3/4). In terms of vulnerability analysis, VA has an increasing trend in the number of investigations related to the use of virtual currencies and virtual assets by criminal organizations (not just cyber criminals). The report further notes that the financial sector in the EU is currently not sufficiently equipped with ML/TF regulatory guidance on the topic of VA. For this reason, the level of terrorist financing vulnerability in relation to virtual currencies is considered to be significant to very significant (3/4).

The analysis of responses of Slovak banks shows that two banks identified customers who provided VA services (Virtual Asset Service Providers - VASP) in the assessed period, the number of customers ranging from 5 to 10. The other banks indicated that they did not have econofrom entering into a business relationship with VASP customers due to a high or unacceptable ML/TF risk. Banks usually identify Virtual Asset Service Providers (VASP) through a combination of due diligence and transaction monitoring. Three banks have implemented procedures for VASP customers in the AML Programme and these customers are categorised within a high ML/TF risk. The other banks do not have such procedures because they do not accept VASP customers or refer to group-wide policies.

Banks that would accept the VASP of customers as part of their AML policy outlined the procedures for exercising due diligence as follows: i.) prior approval of the AML department is required for entering into a business relationship, ii.) entering into a business relationship only in the physical presence of the customer at the bank, iii.) completing a specialised AML questionnaire and providing other information and documents necessary for an adequate ML/TF risk assessment, iv.) gathering detailed information to understand the nature of the VASP's business and ascertain the customer's reputation, v.) evaluating ML/TF control

mechanisms in relation to VASP customers, vi.) verifying reputation based on information available from multiple sources, vii.) increasing the frequency of transaction monitoring, and viii.) increasing the frequency of business relationship reviews by the AML department. Banks also ascertain how VASP customers have set up their own control mechanisms vis-à-vis their customers. Verification of VASP control mechanisms is an important element of the due diligence process in terms of mitigating ML/TF risks related to the fact that VASP customers can have customers in their portfolios that support terrorist financing. Banks have confirmed that VASPs have insufficient processes for managing ML/TF risks in relation to their customers, particularly in the areas of: i.) identifying and verifying the identity of the customer or beneficial owner ii.) determining whether the customer or beneficial owner is a politically exposed person or a sanctioned person iii.) identifying the origin of funds used to purchase VA, iv.) not having mastered ML/TF risk management processes.

After evaluating this information, they will usually refuse to cooperate with VASP. Overall, after evaluating the responses, it can be concluded that banks have set a prudent and conservative approach to VASP and have adequate control mechanisms for the risks they are exposed to in this area.

However, in the future, more attention will need to be paid by supervisory and control authorities to this topic and to the education of entities. Vulnerabilities include the high dynamics of development and technological change in this area, the absence/lack of regulation, the anonymity of the environment, the possibility of cross-border provision of services, the difficulty of understanding VASP technologies by supervisors and control authorities.

De-risking

The Financial Action Task Force (FATF) defines de-risking as a state where financial institutions terminate relationships or do not provide services **to certain types and entire categories of customers** in order to avoid risks, rather than managing and mitigating those risks in accordance with a risk-based approach (RBA). The FATF methodology requires FIs to terminate/reject customers only **after an individual comprehensive risk assessment of each and every customer.** Thus, rejecting customers in whole groups/types is not in line with the RBA.

Around 20% of banks reported that they did not apply de-risking. The remaining around 80% apply de-risking more or less. The banks that gave examples of de-risking mainly mentioned the following situations: i.) customers from high-risk countries (Iraq, Iran, DPRK, Syria), ii.) customers - embassies from sanctioned countries, iii.) customers from outside the EU, iv.) shell banks, v.) online gaming venues, lotteries, unlicenced lotteries, vi.) VASP, vii.) MVTS (Money or Value Transfer Services), viii.) arms trafficking, ix.) pornography industry, x.) projects that have a negative impact on the environment, on human rights violations, etc.

In terms of numbers of customers affected by de-risking, ten banks also reported numbers of customers. The numbers are relatively wide ranging: from 3 customers to 2,000 customers per year. Overall, the numbers roughly average in the tens of customers per year, which is minimal compared to the total number of customers in the banks.

It can be stated that banks assess risks (according to risk factors: customers, business, geography) prudently. The problem of de-risking must be seen in a comprehensive way. On the one hand, the methodological perspective of the bodies that develop global standards for AML/CFT must be respected, while on the other hand the actions of banks that are exposed to risks and bear direct responsibility for the effective and efficient management and mitigation of these risks must also be taken into account. When considering ML/TF risks related to de-risking, the main concern is a situation where all financial institutions would follow the same practice - i.e. they would reject a certain group of customers as a whole and these would eventually be forced to cooperate with illegal, unregulated financial institutions and schemes, thereby increasing the ML/TF risk. On balance, it can be noted that in the banking sector - despite the fact that the majority of banks have indicated that they are de-risking - it can be concluded that a risk of this magnitude has not occurred.

On the other hand, however, banks will need to be educated and stressed that they should treat customers on a case-by-case basis when assessing risks. In particular, it will be necessary to find out how banks proceed in designing the policy for ML/TF risk management and in the risk assessment itself: whether they assess that the whole group of customers is unacceptable for the bank or take into account each customer from a specific risk group on an individual basis. In the context of de-risking, it should be stressed that there is as yet no binding legal regulation at EU level.

Terrorist financing risk management (TF)

Information sources for identifying and managing TF risks

Banks use a number of resources to manage TF risks. Domestic ones are, for example: the FIU SR, the NBS, the MI SR, the Ministry of Foreign and European Affairs of the SR. Foreign: EU legislation, Moneyval, EBA, FATF, OFAC, Worldcheck dtb, systems from parent banks, etc. Banks have their own vetting system based on checking lists of countries, persons, etc. The breadth of sources is related to the business model, the size of the bank, the number of customers (especially non-residents, who are thoroughly vetted).

Models and scenarios of TF risk management

Most banks use specific (i.e. different from ML) scenarios and management models aimed exclusively at managing TF risks. They are generally based on a combination of the use of their own and parent scenarios, models. Their essence lies in assessing mainly geographical risks (high-risk countries, countries where terrorist groups operate), for non-residents they examine the relationship with the Slovak Republic and the justification for establishing accounts in the Slovak Republic. An important part of the process is also the monitoring of transactions - especially to/from risk countries, etc.

Twelve banks identified risks related to TF. Generally, these customers were: i.) non-residents with links to risky third countries, ii.) non-profit organisations that wanted to send money to Middle Eastern countries or had other links to the region, iii.) military equipment dealers, iv.) students with links to high-risk third countries, v.) customers with a combination of a risky business model and links to risky countries, etc. It can be concluded that banks have

adequate tools within their screening and control processes to identify customers with whom potential TF risk is associated. Banks thoroughly screen customers for sanctions lists. Banks thoroughly screen customers for sanction lists. In this regard, it should be noted that over-reliance on screening customers through sanctions lists may also be considered a vulnerability in the context of terrorist financing and therefore - in addition to the rigorous screening of individuals on sanctions lists - attention should also be paid to high-risk individuals outside the sanctions lists who may be linked to individuals on sanctions lists. Banks should therefore screen such persons against the widest possible range of publicly available databases and sources.

In analysing TF-related risks, the assessment team also focused on banks' perceptions of non-profit organisations (NPOs), as some types of NPOs may be potentially vulnerable to diversion for terrorist financing. Banks perceive NPOs as a riskier segment of customers, they have a more attentive perception of them. About 30% of banks have set specific procedures for NPOs and have placed them in a higher risk category. About a quarter of the banks provide NPOs with enhanced due diligence, mainly consisting of: i.) detailed investigation of the purpose for the business relationship, ii.) investigation of the nature of their activities, especially the sources of funding (donor monitoring), iii.) monitoring of their payments, iv.) careful ascertainment of beneficial owners, v.) tracking of the recipients of their payments (geographic aspect of payment monitoring).

The above approach of banks can be assessed positively as prudent in terms of precautionary measures for TF.

The analysis of risks related to NPOs has also taken into account the conclusions of the 2019 EU Supranational ML/TF Risk Assessment Report (chapter Non-profit organisations, page 226 onwards). The analysis shows that there are ML/TF threats at the "significant" level for NPOs (level 3 on a 4-level scale), but for NPOs funding from EU institutions the threat is "low" (1/4). Vulnerability of NPOs to ML/TF is at the "medium" level (2/4), but in the case of NPOs funding from EU institutions, the vulnerability is "low" (1/4).

In the conditions of the SR, it would be advisable for the competent state authorities to establish and publish a list of NPOs for which a higher risk related to terrorist financing can be assumed and also a list of NPOs with a lower risk related to terrorist financing.

In addition to the risks associated with NPOs, the assessment team also focused on how banks approach cash withdrawals in war zones as a potential risk of TF. One-third of banks have set up specific systems to detect ATM withdrawals in war conflict zones. Withdrawal attempts are automatically rejected, or the bank reports them directly to the FIU SR, or the customer is contacted to explain the intercepted business transaction. Other banks have monitoring of ATM withdrawals as part of transaction monitoring.

The assessment team also looked at how banks analyse non-cash transactions to war zones. A quarter of the banks identified customers who had transacted into war zones. Banks have set up the following procedures for these situations: i.) in case of identification of payment to/from Syria, it rejects it (returns the payment to the account of the payer), ii.) in case of Libya and Iraq, the payment is verified and executed only after the necessary information has been

provided to exclude the risk of TF (the bank requests all the necessary information and documents: invoice, documentation of the purpose of the payment - whether it is not military material, information on the beneficial owner of the payee), iii.) the payments are manually verified by the AML department and only after excluding the risk of TF, the payment is released. It can be concluded that banks have developed adequate procedures to manage the risks associated with transactions to high-risk countries in war conflict zones.

Analysis of feedback from banks on the level of ML/TF legislation and regulation

As part of the analysis, the assessment team investigated whether banks consider the current ML/TF legislation to be sufficient. The vast majority of banks (90%) responded positively, some of which would like to see improved regulation and better feedback from domestic authorities. Three banks directly stated that there are a number of contentious (unclear) areas in Act No. 297/2008 Coll. in particular that they would like to see improved. These include: i.) identification and definition of PEP, ii.) definition and practice for determining the beneficial owners (identification and verification of identification), iii.) refinement of procedures for managing cash-related risks (cash management), iv.) refinement of procedures for managing ML/TF risks, v.) refinement of procedures for managing ML/TF risks, vi.) they would welcome assistance from regulators by developing guidance (frequent questions/answers on partial ML/TF issues could be addressed through shared opinions, e.g. the so-called FAQ platform), vi.) they would welcome an implementing regulation for the area regulated by Act No. 297/2008 Coll. (which would define in more detail the procedures expected in the implementation of individual, often controversial provisions of the Act), vii.) from the point of view of the practical application of the Act, there is a lack of interpretation of some provisions of the Act (either in the form of guidelines or binding opinions), viii.) in relation to the area of UTs, banks would welcome more detailed feedback in the context of further UT reviews (e.g. by LEAs), so that they can better incorporate the identified risk factors into their customer profiles, or use this experience with other customers.

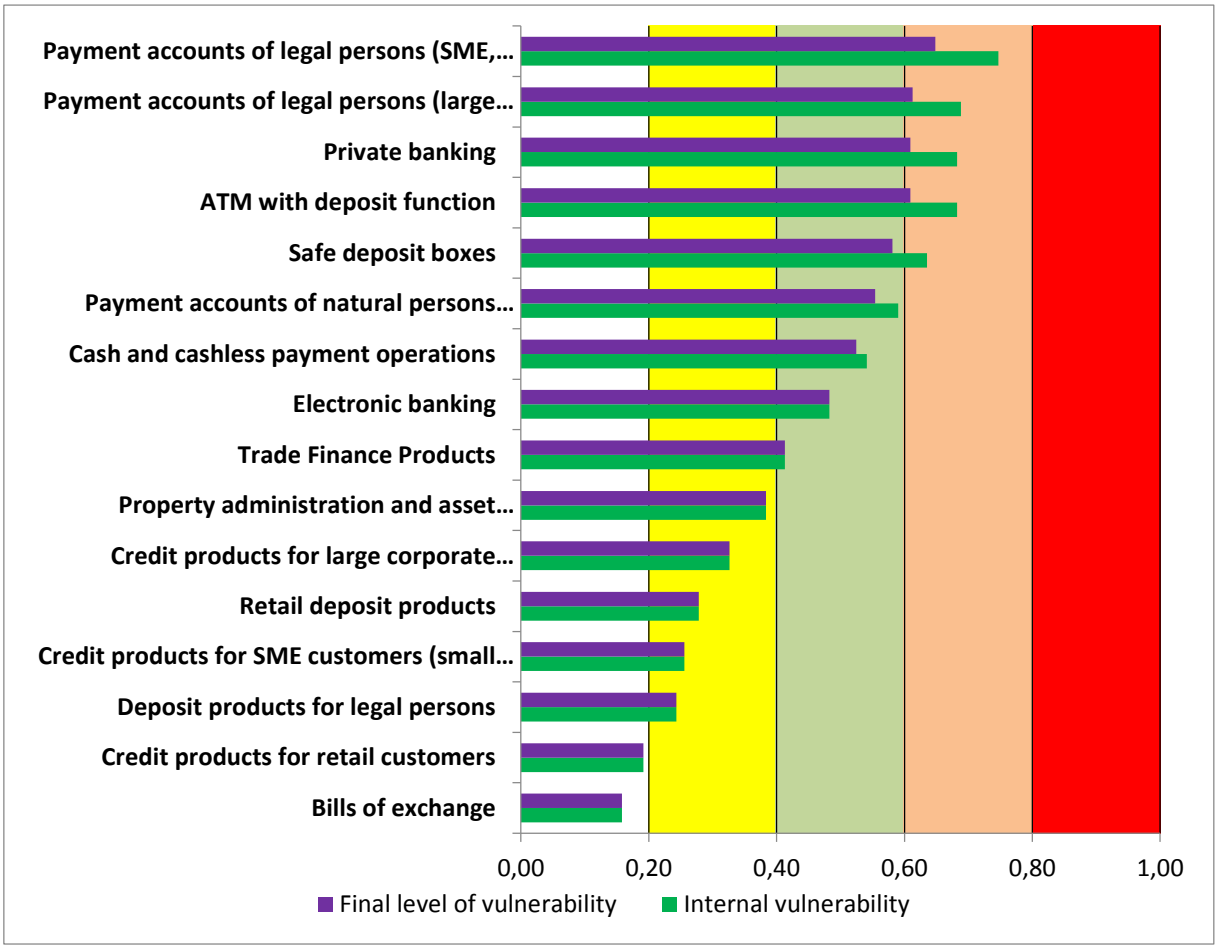
The above-mentioned areas can be perceived as vulnerabilities; therefore, it will be necessary to prepare a mechanism for providing feedback to supervised entities on the basis of regular communication with the entities (e.g., through the SBA, or commissions with the participation of the FIU SR, the NBS, the SBA, banks, etc.).

PRODUCT VULNERABILITY

In order to objectively assess the vulnerability of banking sector entities, a detailed assessment of the products and services provided is essential. The results of such an assessment are crucial in identifying potential vulnerabilities in the products and services provided by banking sector entities. These results are also an important element in the design of risk-based supervision or control.

The assessment of the individual products was based on the following risk scale:

	VULNERABILITY LEVEL				
Product vulnerability:	**Low**	**Medium-low**	**Medium**	**Medium-high**	**High**
Vulnerability interval according to the World Bank	**0.0-0.2**	**0.2-0.4**	**0.4-0.6**	**0.6-0.8**	**0.8-1.0**
Risk degree	**1**	**2**	**3**	**4**	**5**



The results of the assessment of the above 16 products within the NRA showed a wide range of vulnerability levels for the individual products and services - from low to medium-high. **A low level of vulnerability, meaning a low risk of a particular product being abused for legalisation purposes, was found for bills of exchange. On the other hand, a medium-high level of vulnerability, which means an increased risk of misuse of a specific product for legalisation purposes, was found for corporate payment accounts (small and medium enterprises).** The final vulnerability level of the above products (risk score) was calculated by the World Bank's assessment module after taking into account the internal vulnerability of the product (internal vulnerability represents the risk score achieved by the product without the impact of ML/TF risk mitigation measures).

In the next section, we provide a more detailed look at products and services with higher levels of vulnerability.

Payment accounts for SMEs

Payment accounts of legal persons for small and medium enterprises are among the most widely used products provided by banks for this group of customers. It is the primary instrument through which funds enter the legal banking system. The product is widely used, provided by 20 banks, it allows daily execution of cash and non-cash transactions (with no limit), both domestic and cross-border, including risky third countries, the product can be used by companies with unclear ownership structure, so-called letter-box companies with links to off-shore zones, etc. The above characteristics can also be seen as risks of this product in terms of ML/TF. As regards SME payment accounts, they are connected with the highest number of UTRs to the FIU SR and the accounts are often used to commit tax and carousel frauds. It can be noted that the risks analysed in the 1st round of NRA continue to persist, in particular the unrestricted limits on cash and non-cash transactions. Another risk factor for this product is the profile of the customer base. In the context of the customer profile, the complicated ownership structure of the companies should also be mentioned as a risk, where it is difficult to clearly identify beneficial owners. The most common transactions carried out through the business accounts of small and medium entrepreneurs are those that are part of carousel frauds or frauds carried out in connection with excessive VAT deductions. Furthermore, cross-border transfers to risky countries or countries referred to as off-shore tax havens often occur. A special category in terms of the customer's "business activity" are business entities engaged in the purposive establishment and dissolution of companies, including letter-box companies, as well as entities using virtual seats of such companies. Approximately 90% of banks rate the product in the higher risk range - medium to high risk. The assessment team assigns the **SME payment account to the medium risk category with a tendency towards high risk (4.5)**.

(Note: The annex contains tables and charts for the period 2011-2019 concerning the volume of cash transactions on accounts of customers - LPs: P7)

Payment account for large corporate customers

The payment account for this group of customers is very similar to the one for SMEs and is used to carry out daily payment operations (both domestic and cross-border) for large companies. Disposal of the account is practically the same as with the SME payment account - using e-banking and payment cards issued to the account, or upon a personal visit of the customer to the bank's branch. The product is widely used, provided by 20 banks, and allows for the daily execution of unlimited cash and non-cash transactions, both domestic and cross-border, including risky third countries. The structure of the customer profile is different from that of SMEs. Owners are large companies that have established organisational structures, compliance and audit departments, have internal risk management policies, codes. On the other hand, some have links to off-shore zones or tax havens. Approximately 50% of banks rate the product as medium risk, 41% of banks perceive the product as medium-high risk. **The assessment team rated the product as medium risk (4.0).**

(Note: The annex contains tables and charts for the period 2011-2019 concerning the volume of cash transactions on accounts of customers - LPs: P7)

Private banking (PB)

This product (service) is currently provided by seven banks. It can be characterised as the provision of a highly superior service to important and creditworthy customers with a product offering that is highly customised to the individual customer's requirements.

Active use of the product is generally associated with a high degree of discretion and a close working relationship between the customer and the private banker, which may contribute to increasing the risks associated with tax optimisation. Other risks are related to the still high use of cash for this product (service), and one of the persistent risks is the low level of reporting of unusual transactions of PB customers. The analysis shows a fairly even spread in the assessment of PB vulnerability: 2 banks reported high, 2 banks reported medium-high, 2 banks reported medium, and 1 bank reported medium-low risk.

For PB, the assessment team also took into account the conclusions of the EU Supranational ML/TF Risk Assessment Report (Chapter 5 Private Banking). The report shows that the risk of ML and tax criminal offences is high, precisely because of the combination of sophisticated products, their complexity and also the solvency profile of customers (often PEPs). Another risk that the report notes is the very low (almost non-existent) level of UT reporting for PB customers. This negative trend is also noted by the assessment team in the conditions of the SR. For PB, the ML risk is rated as significant to very significant (3/4) in the report.

It can be noted that banks providing PB perceive the rated product in the medium to medium-high risk category. Even taking into account the persistent product risks mentioned above in the detailed risk analysis of the PB product, the assessment team shares the banks' view and rates the product as **medium-high risk** (4.5).

Safe deposit boxes SDB

The assessment team analysed the product in detail as a banking service in the section of other ML/TF risks. In this section, the assessment team focused on completing the assessment and also took into account the findings from the 2019 EU Supranational ML/TF Risk Assessment Report (Chapter 18). The report shows that ML risks are significant, in particular because of the possibility to hide the proceeds of crime without detection. These "dormant" deposit systems are increasingly being used to store deposits and withdraw money from the financial system, according to law enforcement authorities. The report identifies the ML risk level as significant (3/4).

In the conditions of the SR banks rate the product as medium-high with a bias towards high risk. The assessment team concurred with the banks' assessment and considers **SDBs to be medium-high risk** (4.0).

Payment accounts for natural persons

Payment accounts for natural persons - like payment accounts for SMEs and large corporate customers - are among the most important and widespread products provided by banks for this group of customers. It is the primary instrument through which funds enter the legal banking system. The ML/TF risks arising from the unlimited cash and non-cash transaction options are similar to those of SME and corporate payment accounts, however, the customer base profile can be considered less risky, but the trend of high use of accounts for cash transactions persists. In total, 16 banks provide the product. Up to 70% of banks rate the risk of the product as medium. The rest of the banks rate the product as medium-low risk. **Overall, banks rate the product as medium risk (3), the assessment team rated the product slightly higher as medium-high risk (3.5).**

(Note: For the volume of cash and non-cash transactions in the accounts of natural persons, the following tables and charts for the period 2011-2019 are attached: P6 and P8)

For other products such as bills of exchange, property administration and asset management services, corporate loans (SME and large corporate customers), retail loans, corporate and retail deposit products, etc., the assessment team agreed with the banks' view. This group of products is in the low or medium-low risk range (2-3). This is mainly due to the thorough scrutiny of customer documents prior to product delivery (especially for loans, bills of exchange and trade finance), and also for deposit products.

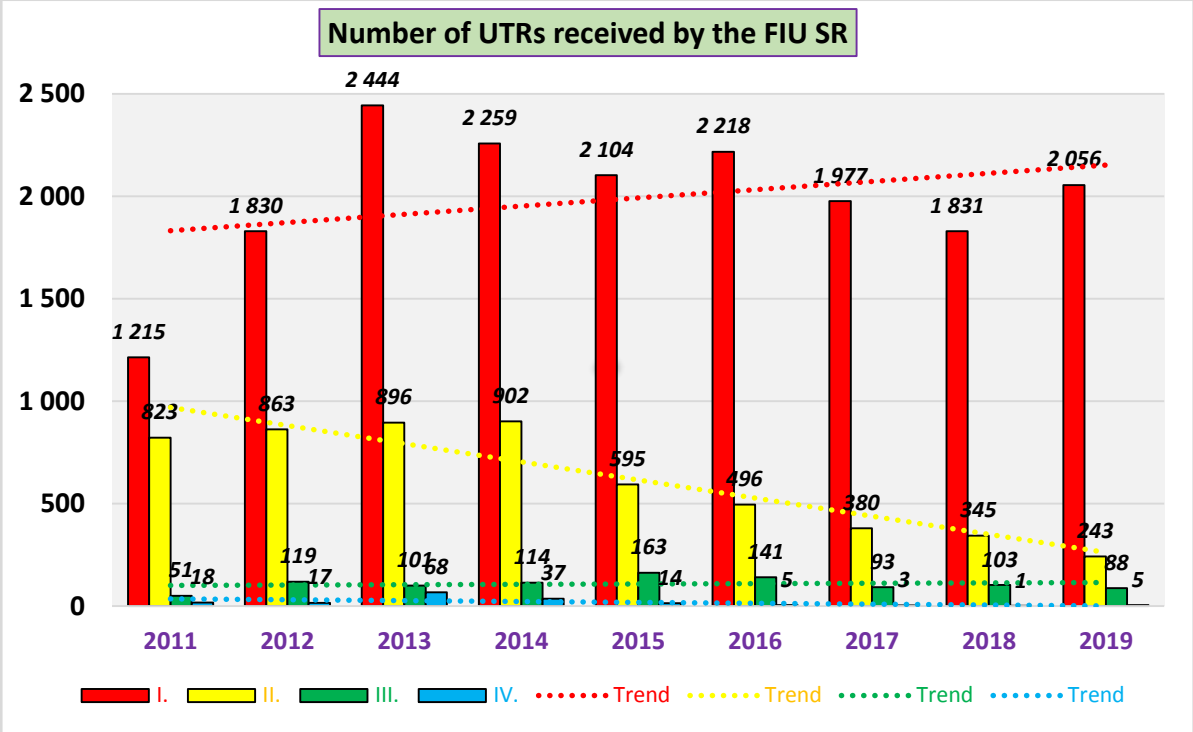
Products such as non-cash payment transactions and e-banking are perceived by both banks and the assessment team as medium risk (3). Before providing a product to a customer, banks thoroughly verify the customer and obtain necessary information within due diligence. On the other hand, there are still risks associated with the characteristics of these products, in particular the possibility of unrestricted transactions, including transactions into risky areas. In this context, the assessment team rates the product as medium risk (3).

ATM deposits:

ATM deposits can be considered a relatively new product that was not assessed in the 1st round of NRA. To mitigate the risks associated with ATM deposits, banks have taken the measures described above in the analysis of risks associated with cash operations. Most of the measures relate to post-transaction monitoring of ATM deposits. In the case of ATM deposits, banks do not have direct contact with the customer, as in the case of a deposit at a bank's branch, nor do they have the ability to determine the origin of the funds directly at the time of the customer's deposit, nor other related information that would help the bank assess the risks of a given transaction (e.g., the reason for the deposit, the next use of the funds, etc.). The assessment team therefore considers this type of product to be medium risk (4) and agrees with the banks' assessment (4).

Number of UTRs received from banks by the FIU SR

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total in %: 2011-2015 (5 years)	Total in %: 2016-2019 (4 years)	Total in %: 2011-2019 (9 years)
I.	1 215	1 830	2 444	2 259	2 104	2 218	1 977	1 831	2 056	67,3	80,9	72,8
II.	823	863	896	902	595	496	380	345	243	27,9	14,7	22,5
III.	51	119	101	114	163	141	93	103	88	3,7	4,3	4,0
IV.	18	17	68	37	14	5	3	1	5	1,1	0,1	0,7
Total	*2 107*	*2 829*	*3 509*	*3 312*	*2 876*	*2 860*	*2 453*	*2 280*	*2 392*	*100,0*	*100,0*	*100,0*

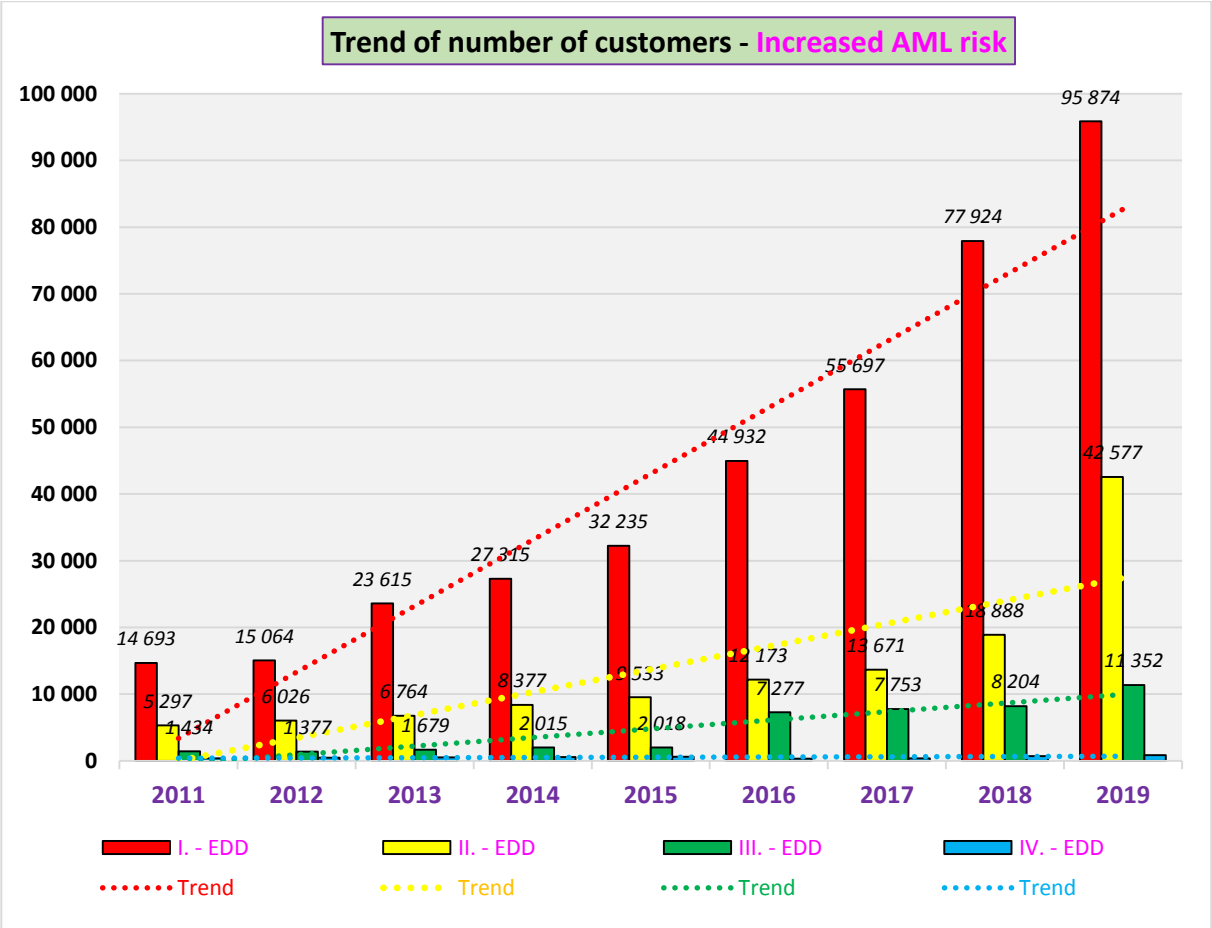


Note: The UTRs from the NBS are not included in the total number of UTRs received by the FIU SR.

Number of UTRs received by the FIU SR for the period of the 1st and 2nd NRA has a slightly increasing tendency for banking group I, on the contrary, a more significant decrease has been observed for banking group II, banking group III has a balanced tendency and banking group IV has a decreasing tendency. In terms of the number of UTRs received by the FIU SR from all banks, banking group I had a share of almost 73%.

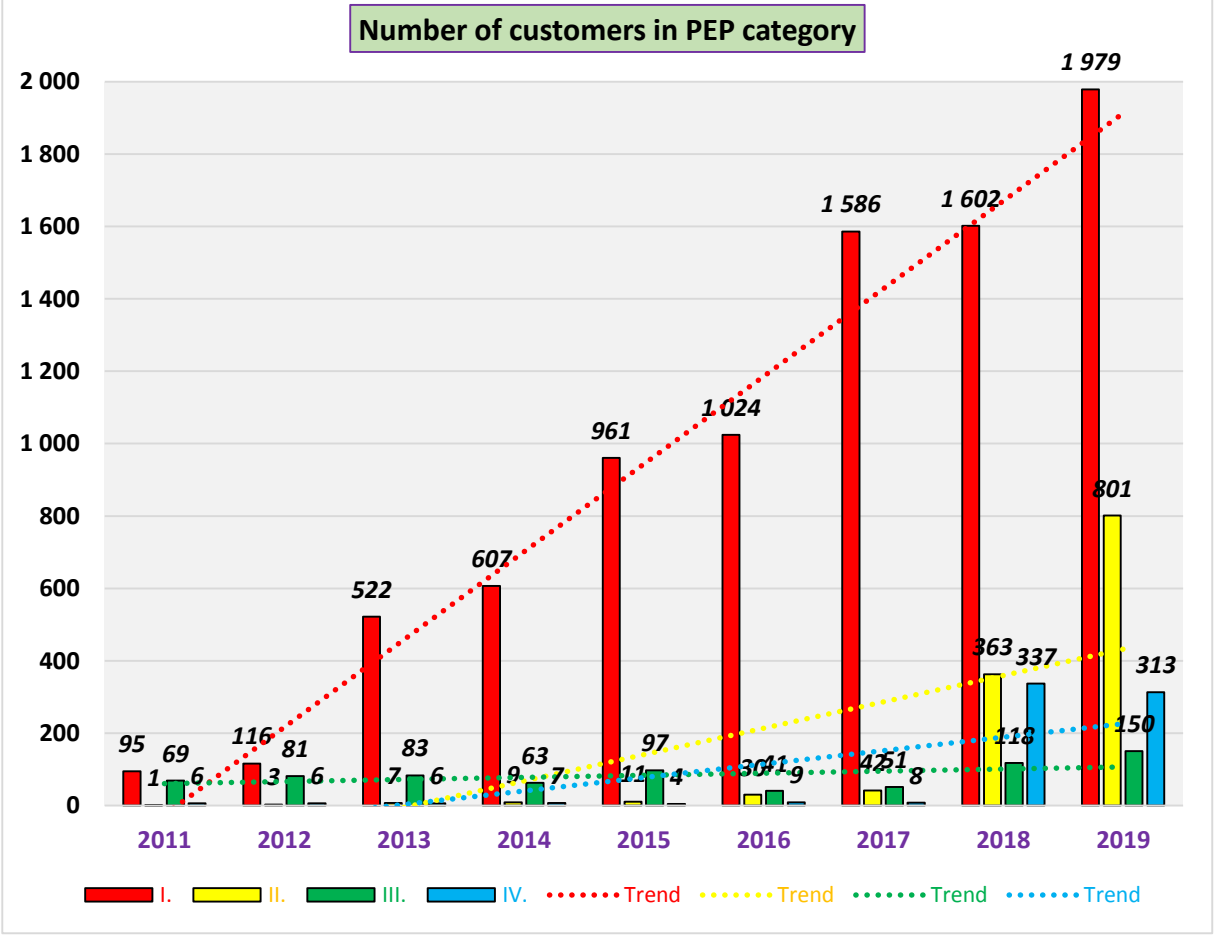
Number of customers – Standard/increased AML risk (provision of basic/enhanced due diligence)

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019	Ratio CDD/EDD 2015 (in %)	Ratio CDD/EDD 2019 (in %)
I. - CDD	3 547 160	3 524 286	3 538 188	4 806 131	4 683 865	4 677 145	4 641 376	4 783 647	4 834 080	99,32	98,06
I. - EDD	14 693	15 064	23 615	27 315	32 235	44 932	55 697	77 924	95 874	0,68 ↗	1,94
II. - CDD	1 534 799	1 617 889	1 687 746	1 696 363	1 704 775	1 696 889	1 766 772	1 768 844	1 756 934	99,44	97,63
II. - EDD	5 297	6 026	6 764	8 377	9 533	12 173	13 671	18 888	42 577	0,56 ↗	2,37
III. - CDD	314 746	387 176	327 410	394 672	457 636	446 915	490 643	511 828	525 650	99,56	97,89
III. - EDD	1 434	1 377	1 679	2 015	2 018	7 277	7 753	8 204	11 352	0,44 ↗	2,11
IV. - CDD	1 017 920	1 026 709	1 014 078	984 356	948 132	913 575	890 978	849 194	826 621	99,94	99,90
IV. - EDD	361	480	515	557	592	331	357	695	860	0,06 ↗	0,10
CDD total:	6 414 625	6 556 060	6 567 422	7 881 522	7 794 408	7 734 524	7 789 769	7 913 513	7 943 285	99,43	98,14
EDD total:	21 785	22 947	32 573	38 264	44 378	64 713	77 478	105 711	150 663	0,57 ↗	1,86



The number of customers that the banks had under enhanced due diligence - EDD for the period of the 1st and 2nd NRA in all banking groups had an upward trend, with the most significant increase in banking group I and banking group II, especially in 2019. Comparing the proportion of customers in standard and enhanced risk at the end of 2015 and 2019, it can be noted that there has been an increase in the number of customers maintained in EDD. The above phenomenon could be mainly caused by the fact that there has been a better/more realistic risk assessment of customers by banks after the 1st NRA. Thus, the comparison of the average share of EDD customers to CDD customers was about 2%/98% in 2019 (the share of EDD customers in banks should continue to be close to the real riskiness of the banking customer base).

Number of customers in PEP category												
Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total in %: 2011-2015 (5 years)	Total in %: 2016-2019 (4 years)	Total in %: 2011-2019 (9 years)
I.	95	116	522	607	961	1 024	1 586	1 602	1 979	83,6	73,2	75,8
II.	1	3	7	9	11	30	42	363	801	1,1	14,6	11,3
III.	69	81	83	63	97	41	51	118	150	14,3	4,3	6,7
IV.	6	6	6	7	4	9	8	337	313	1,1	7,9	6,2
Total:	171	206	618	686	1 073	1 104	1 687	2 420	3 243	100,0	100,0	100,0

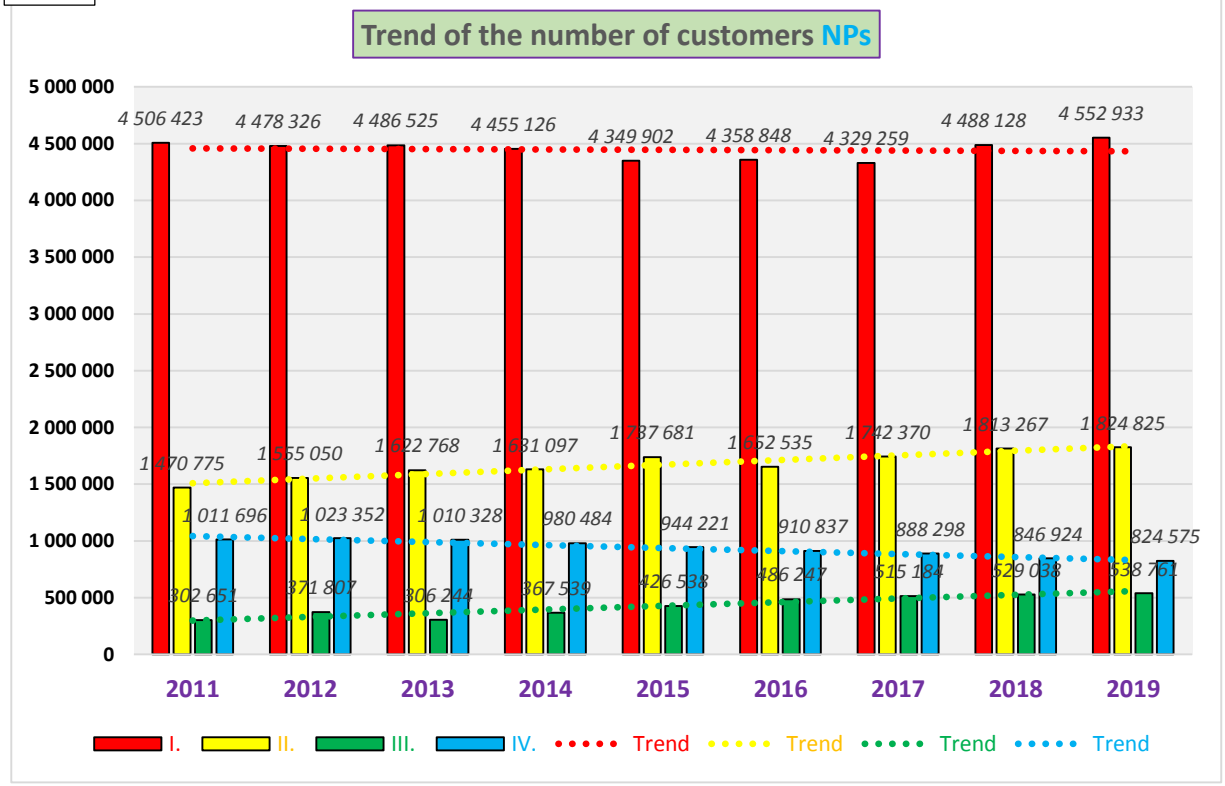


Number of customers in the PEP category for the period of the 1st and 2nd NRA had an upward trend in all banking groups, with the most significant increase in banking group I. Banking groups II and IV saw an increase in PEPs especially in 2018 and 2019 which could be mainly due to the adoption of the amendment to the AML Act in 2018 (when domestic PEPs were tracked).

Number of customers – natural persons (NPs)

Počet klientov - Fyzická osoba (FO)

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019	Share of customers NPs in 2015 in (%)	Share of customers NPs in 2019 (in %)
I.	4 506 423	4 478 326	4 486 525	4 455 126	4 349 902	4 358 848	4 329 259	4 488 128	4 552 933	58,3	58,8
II.	1 470 775	1 555 050	1 622 768	1 631 097	1 737 681	1 652 535	1 742 370	1 813 267	1 824 825	23,3	23,6
III.	302 651	371 807	306 244	367 539	426 538	486 247	515 184	529 038	538 761	5,7	7,0
IV.	1 011 696	1 023 352	1 010 328	980 484	944 221	910 837	888 298	846 924	824 575	12,7	10,7
Total:	*7 291 545*	*7 428 535*	*7 425 865*	*7 434 246*	*7 458 342*	*7 408 467*	*7 475 111*	*7 677 357*	*7 741 094*	*100,0*	*100,0*

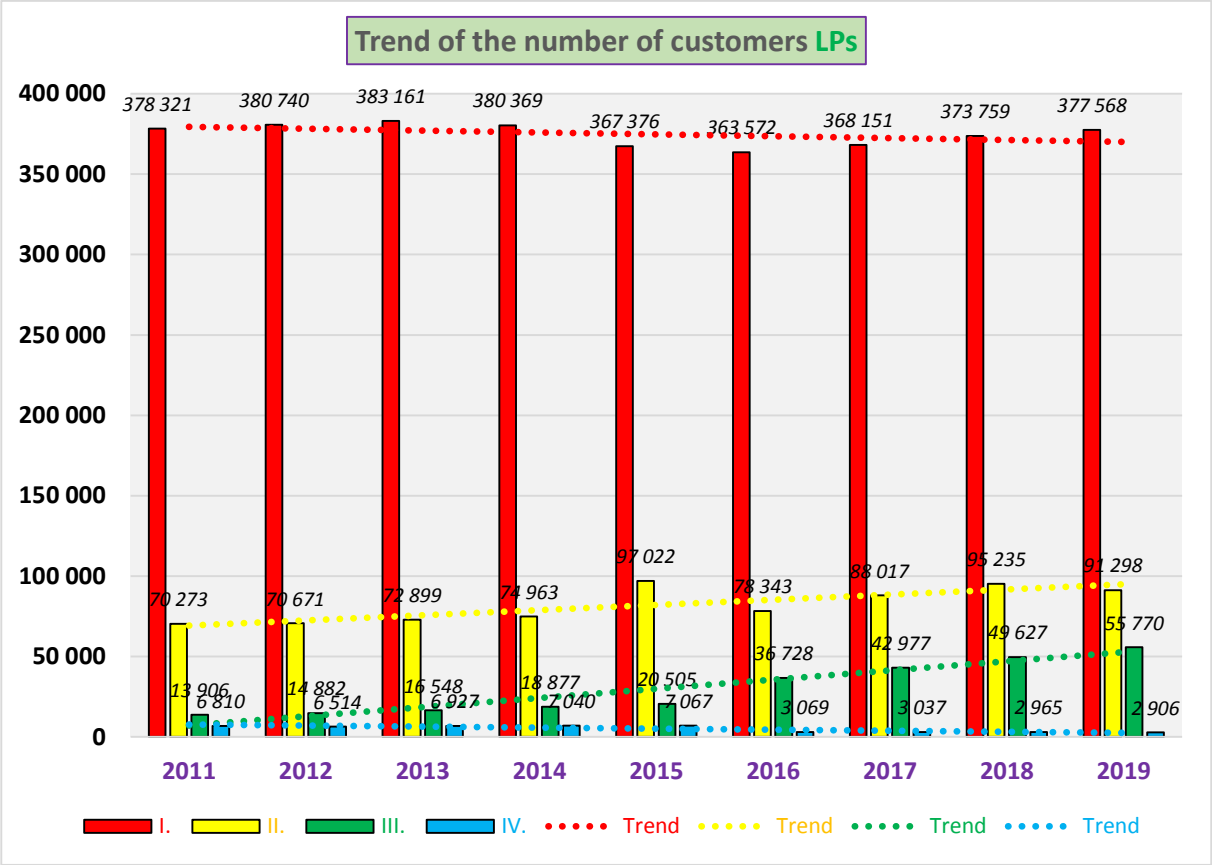


Note: The total number of NP customers included retail and private banking customers

Number of customers - **NPs** for the period of the 1st and 2nd NRA has a stabilised trend in Group I banks, a slightly increasing trend in Group II and Group III banks and a slightly decreasing trend in Group IV banks.

Number of customers – legal persons (LPs)

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019	Share of customers LPs in 2015 in (%)	Share of customers LPs in 2019 (in %)
I.	378 321	380 740	383 161	380 369	367 376	363 572	368 151	373 759	377 568	74,7	71,6
II.	70 273	70 671	72 899	74 963	97 022	78 343	88 017	95 235	91 298	19,7	17,3
III.	13 906	14 882	16 548	18 877	20 505	36 728	42 977	49 627	55 770	4,2	10,6
IV.	6 810	6 514	6 927	7 040	7 067	3 069	3 037	2 965	2 906	1,4	0,6
Total:	*469 310*	*472 807*	*479 535*	*481 249*	*491 970*	*481 712*	*502 182*	*521 586*	*527 542*	*100,0*	*100,0*

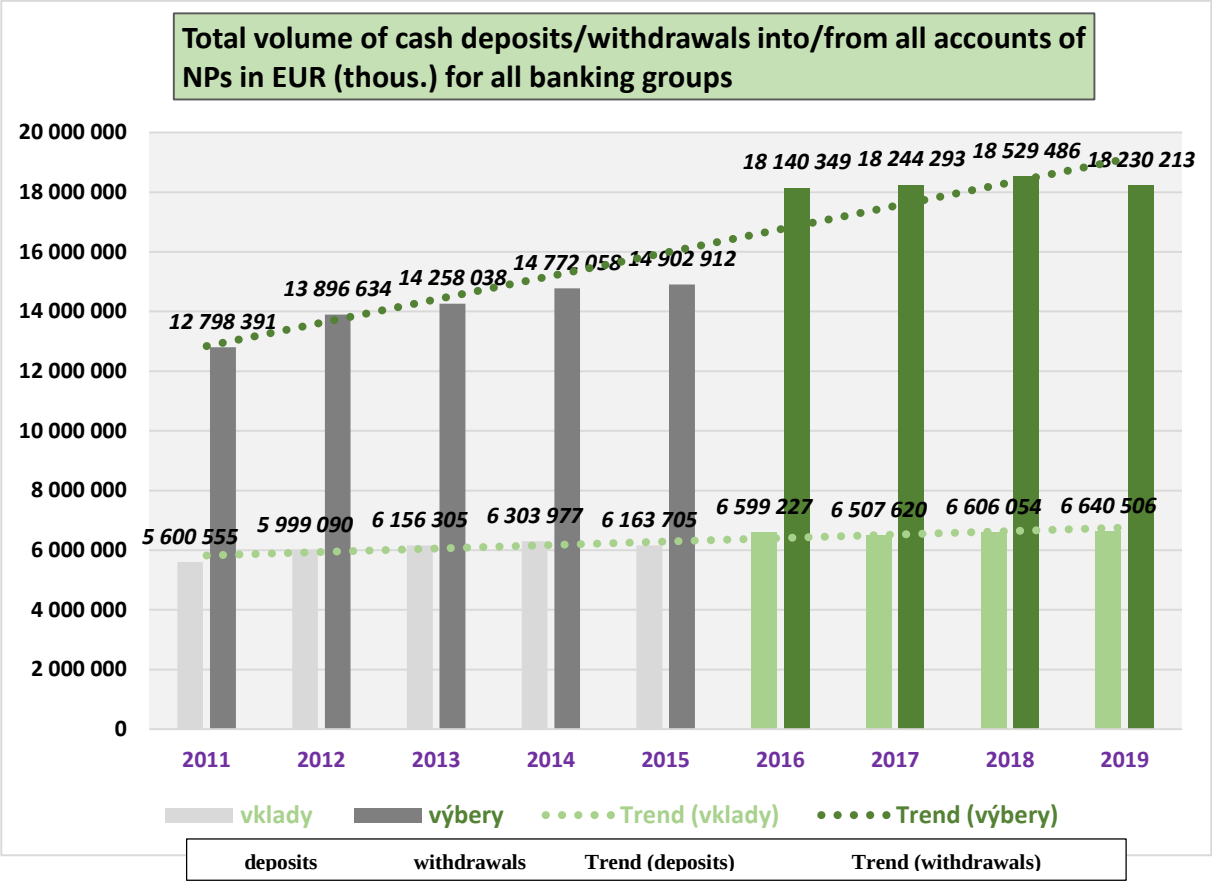


Number of customers - **LPs** for the period of the 1st and 2nd NRA has a stabilised trend in Group I banks, a slightly increasing trend in Group II and Group III banks and a decreasing trend in Group IV banks.

Total volume of cash deposits/withdrawals into/from all accounts of NPs in EUR (thous.)

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019
I. (+)	4 277 396	4 599 365	4 713 222	4 833 871	5 012 020	5 589 077	5 574 915	5 586 558	5 593 728
I. (-)	10 490 976	11 076 417	11 177 450	11 598 549	11 996 578	15 033 616	15 141 589	15 269 556	14 993 918
II. (+)	1 315 883	1 390 494	1 432 672	1 458 756	1 137 982	969 050	875 375	953 414	973 379
II. (-)	2 295 404	2 811 075	3 069 571	3 158 385	2 889 555	2 755 219	2 690 700	2 815 070	2 784 056
III. (+)	7 276	9 232	10 411	11 350	13 702	41 100	57 330	66 082	73 399
III. (-)	12 011	9 142	11 017	15 124	16 779	351 515	412 004	444 861	452 240
IV. (+)	0	0	0	0	0	0	0	0	0
IV. (-)	0	0	0	0	0	0	0	0	0
deposits	***5 600 555***	***5 999 090***	***6 156 305***	***6 303 977***	***6 163 705***	***6 599 227***	***6 507 620***	***6 606 054***	***6 640 506***
withdrawals	***12 798 391***	***13 896 634***	***14 258 038***	***14 772 058***	***14 902 912***	***18 140 349***	***18 244 293***	***18 529 486***	***18 230 213***

Note: (+) =deposits, (-) = withdrawals

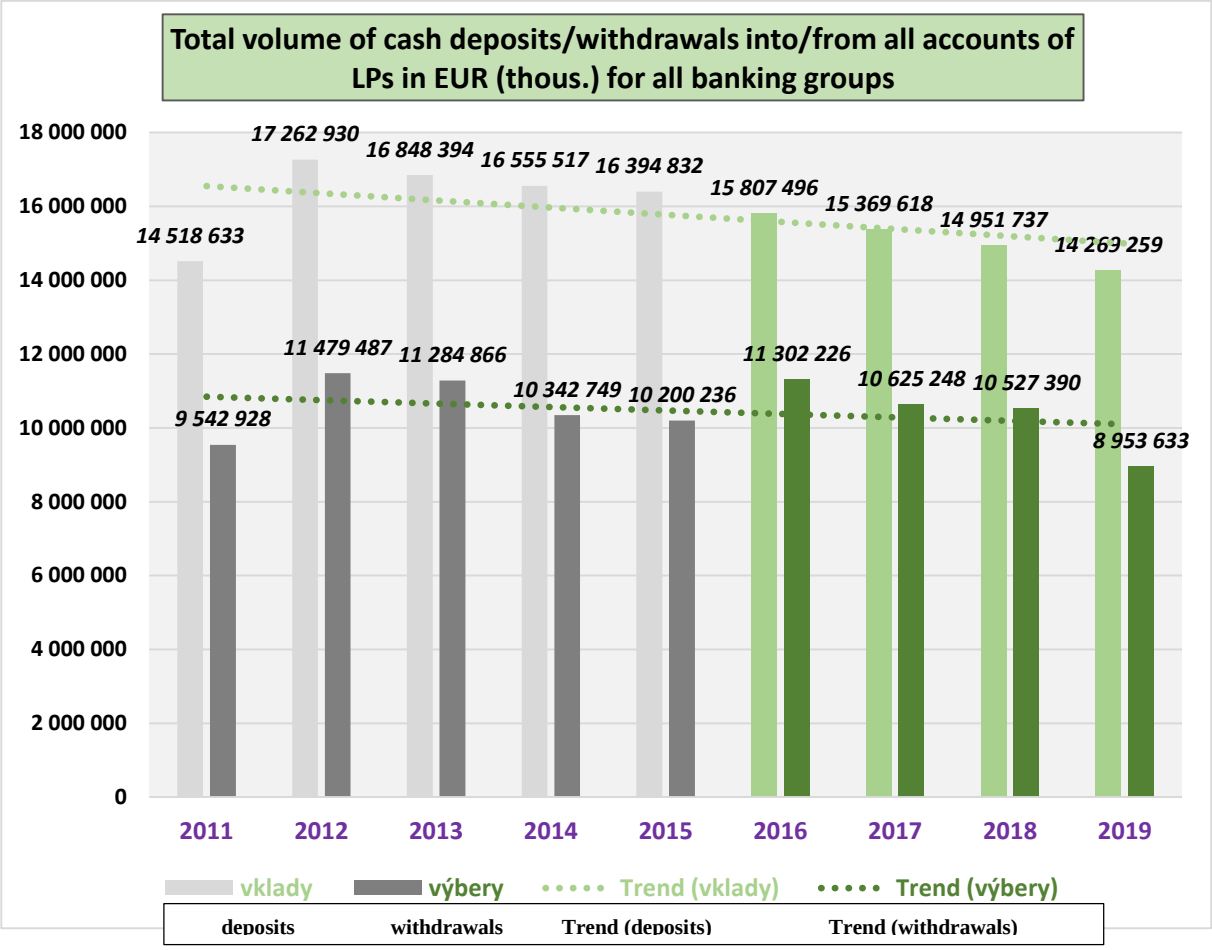


In the period of the 1st and 2nd NRA, cash deposits in the payment accounts of customers – natural persons held in EUR currency recorded a steady tendency in contrast to cash withdrawals, which were made in 2-3 times larger volumes. On the negative side, cash withdrawals in Slovakia from natural persons' accounts appear to be on an upward trend in the long term, although during the 2nd NRA, an almost balanced trend was recorded (the trend of transaction volumes in some EU countries is shifting more to the non-cash area at the expense of cash). For 2019, cash withdrawals in all banks from payment accounts of customers – natural persons reached a volume of about EUR 18.2 billion, which represents about 22% of GDP.

Total volume of cash deposits/withdrawals into/from all accounts of LPs in EUR (thous.)

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019
I. (+)	11 604 908	14 053 481	13 665 751	13 091 299	12 881 640	12 396 193	11 983 452	11 510 917	11 076 388
I. (-)	8 034 794	9 781 013	9 680 231	8 726 267	8 480 412	10 057 835	9 439 198	9 354 173	7 893 207
II. (+)	2 901 819	3 199 527	3 169 246	3 423 409	3 459 774	3 001 917	2 978 499	3 083 193	2 883 857
II. (-)	1 491 998	1 681 164	1 594 258	1 602 148	1 695 803	1 146 272	1 083 160	1 095 174	988 692
III. (+)	11 906	9 923	13 398	40 810	53 418	409 386	407 666	357 626	309 013
III. (-)	16 136	17 310	10 377	14 334	24 021	98 119	102 890	78 043	71 733
IV. (+)	0	0	0	0	0	0	0	0	0
IV. (-)	0	0	0	0	0	0	0	0	0
deposits	*14 518 633*	*17 262 930*	*16 848 394*	*16 555 517*	*16 394 832*	*15 807 496*	*15 369 618*	*14 951 737*	*14 269 259*
withdrawal	*9 542 928*	*11 479 487*	*11 284 866*	*10 342 749*	*10 200 236*	*11 302 226*	*10 625 248*	*10 527 390*	*8 953 633*

Note: (+) =deposits, (-) = withdrawals



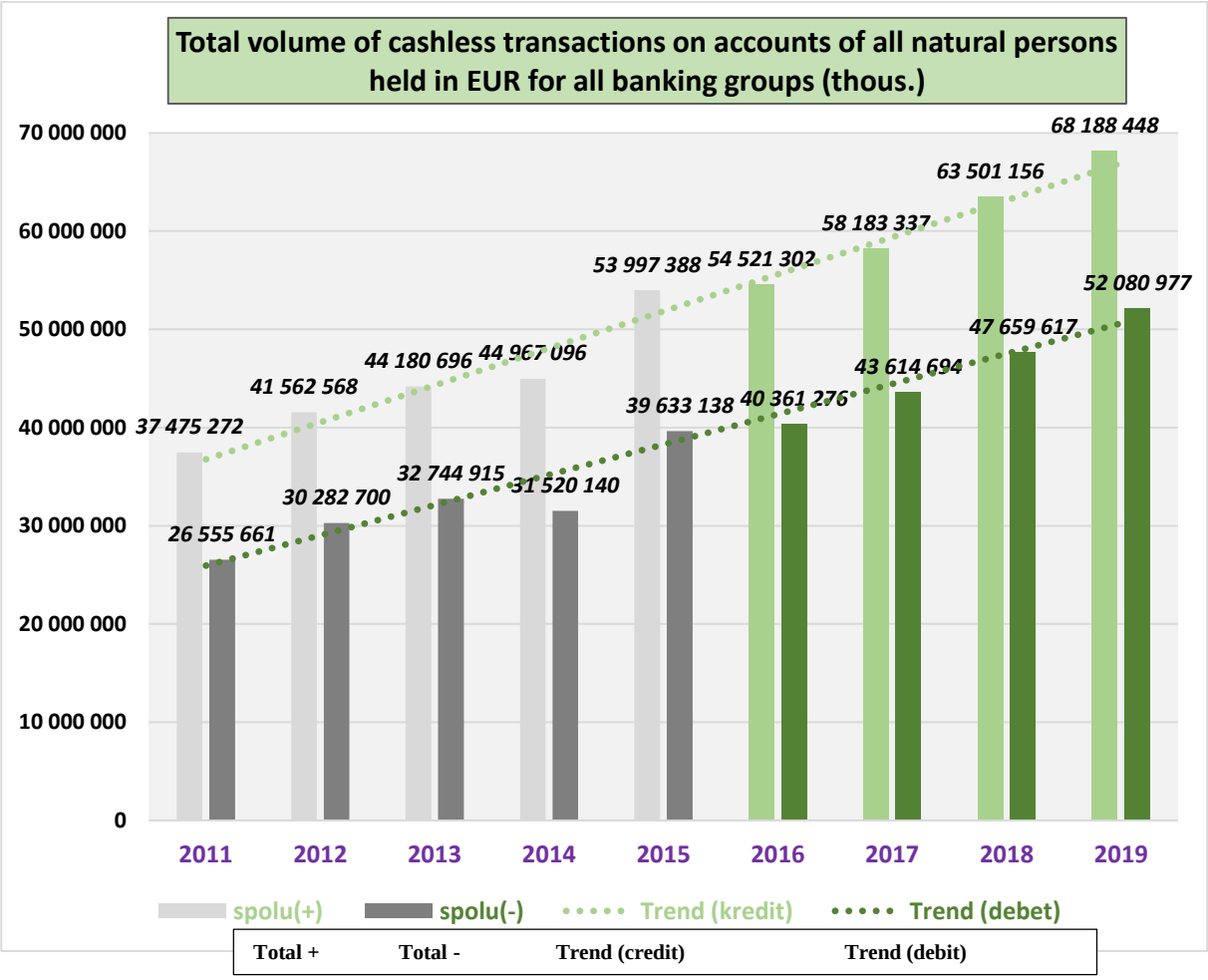
Cash deposits and withdrawals in/from payment accounts of customers – legal persons held in EUR during the periods of the 1st and 2nd NRA had a decreasing trend. Compared to the transactions made through payment accounts of natural persons, a higher share of deposits, as opposed to withdrawals, was recorded in the order of 1.5 times higher volumes. For 2019, cash deposits in all banks on payment accounts of customers – legal persons amounted to about EUR 14.2 billion, which represents about 17% of GDP.

The trend of cash activity in the payment accounts of customers – legal persons decreasing in the long term is a positive development, but cash payments can still be considered a very significant threat and vulnerability in terms of money laundering, and such activity can be largely linked to tax crime in Slovakia.

Total volume of credit/debit cashless transactions on the accounts of NPs in EUR (thous.)

Banking group	2011	2012	2013	2014	2015	2016	2017	2018	2019
I. (+)	27 950 082	31 162 586	32 651 609	35 034 529	42 954 222	42 800 759	45 348 996	48 767 829	52 095 496
I. (-)	19 869 968	22 591 451	24 061 298	24 455 177	31 632 115	29 837 706	32 220 437	34 810 203	38 360 883
II. (+)	5 283 817	5 756 672	6 258 554	6 743 712	7 495 254	8 809 029	9 707 563	11 483 787	12 518 224
II. (-)	2 752 140	2 913 350	3 045 577	3 779 838	3 888 786	7 674 379	8 429 928	9 722 862	10 333 743
III. (+)	3 527 401	3 949 920	4 486 725	2 157 604	2 366 298	1 550 948	1 902 590	2 132 328	2 440 095
III. (-)	3 287 645	4 075 135	4 921 109	2 531 495	3 110 826	1 667 795	1 872 277	2 059 439	2 257 086
IV. (+)	713 971	693 390	783 808	1 031 251	1 181 614	1 360 567	1 224 188	1 117 212	1 134 632
IV. (-)	645 908	702 764	716 931	753 630	1 001 411	1 181 395	1 092 052	1 067 113	1 129 265
Total +	*37 475 272*	*41 562 568*	*44 180 696*	*44 967 096*	*53 997 388*	*54 521 302*	*58 183 337*	*63 501 156*	*68 188 448*
Total -	*26 555 661*	*30 282 700*	*32 744 915*	*31 520 140*	*39 633 138*	*40 361 276*	*43 614 694*	*47 659 617*	*52 080 977*

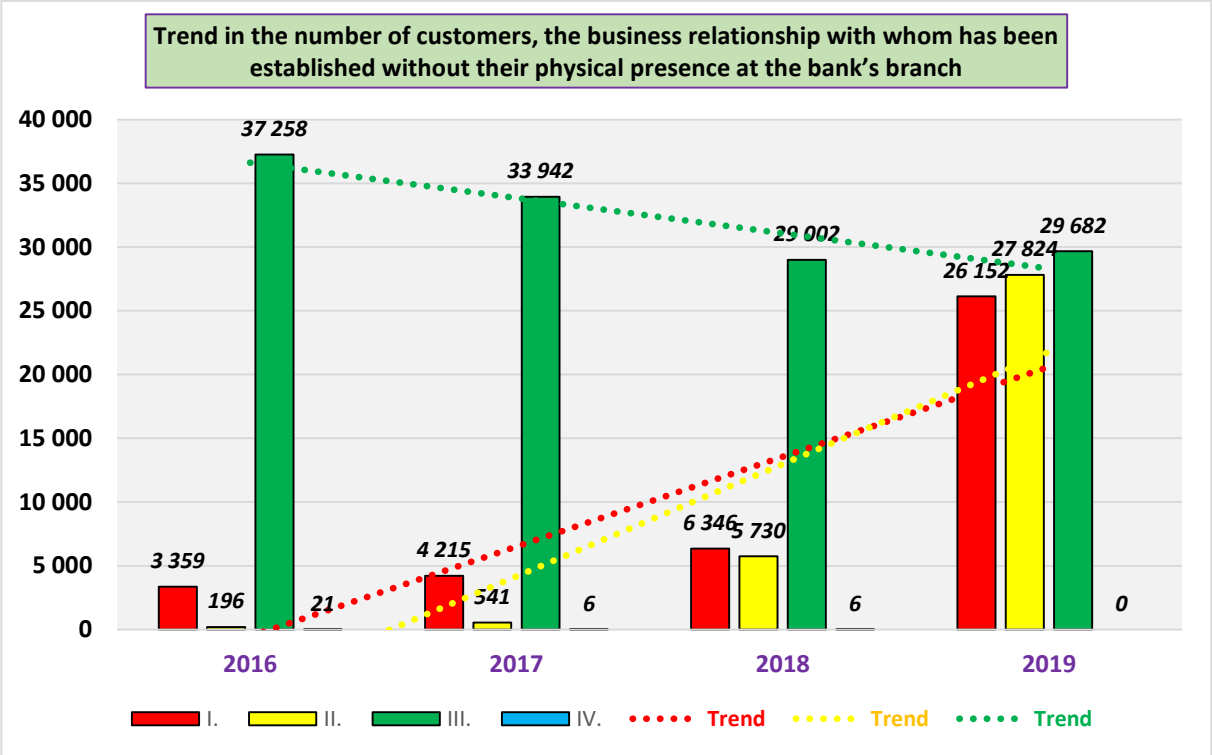
Note: (+) =deposits, (-) = withdrawals



In the period of the 1st and 2nd NRA, the volume of cashless transactions on payment accounts of customers – natural persons held in EUR was increasing which can be considered a natural trend of development.

Number of customers, the business relationship with whom has been established without their physical presence at the bank's branch

Banking group	2016	2017	2018	2019	r.2019 /v %/
I.	3 359	4 215	6 346	26 152	31,3
II.	196	541	5 730	27 824	33,3
III.	37 258	33 942	29 002	29 682	35,5
IV.	21	6	6	0	0,0
Total:	*40 834*	*38 704*	*41 084*	*83 658*	*100,0*



The number of customers for whom an account has been opened without physical presence at a branch is on an increasing trend in Group I and II banks, while the number of customers for whom an account has been opened without physical presence at a branch is on a slightly decreasing trend in Group III banks. A significant increase was recorded in 2019, which was mainly due to the massive promotion of such a way of acquiring clients (establishing a business relationship remotely) by some banks.

9. SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

For the non-financial sector, the following occupations and activities have been assessed from the perspective of AML risk for NRA for the years 2016 to 2019:

lawyer, notary, court distrainor, auditor, tax advisor, accountant, postal undertaking, gambling operator, legal person or natural person authorised to mediate sale, lease and purchase of real estate, organisational and economic advisor, provider of services to commercial companies, legal person or natural person authorised to deal in precious metals or precious stones.

9. Vulnerability assessment and analysis of the whole non-financial sector in terms of the identified assessed variables.

In assessing the vulnerability of the non-financial sector, the working group assessed the following variables and came to the following conclusion:

9.1.1. Comprehensiveness of legal regulation.

The comprehensiveness of legal regulation is a variable that includes, on the one hand, the obligations arising for the obliged entity from Act No. 297/2008 Coll., as well as the right to obtain the necessary data from the customer and, on the other hand, the obligation of the customer to provide the necessary data and information in case they want to be a customer of the obliged entity. Within this variable, the authorisations and possibilities of the FIU SR were also evaluated. All the tasks of the SR resulting from the directives of the European Parliament and of the Council (EU), which have been approved so far, concerning the issue of legalisation of proceeds of crime and terrorist financing, have been transposed in current Act No. 297/2008 Coll.

9.1.2. Efficiency of surveillance/supervision.

The FIU SR is the only supervisory authority over the non-financial sector, with the exception of the gambling operator sector, where the supervision over the legalisation of proceeds of crime and terrorist financing was also carried out by the Ministry of Finance of the Slovak Republic, the Financial Directorate of the Slovak Republic, the Tax and Customs Office and, as of 1 June 2019, the newly established Gambling Regulatory Authority (hereinafter referred to as the "GRA"). The FIU SR has adequate authority to control compliance with measures against the legalisation of proceeds of crime, has a good understanding of the risks involved, carries out inspections, imposes fines for non-compliance with obligations, and issues guidelines as required by the obliged entity. An insufficient number of employees of the Financial Intelligence Unit supervising this sector has been identified in this area.

The reduced effectiveness of supervision in the period under assessment was recorded in the non-financial sector, namely in the free trade licences, where the inspection was not allowed to be carried out and the highest number of financial penalties was imposed for failure to provide assistance during the inspection. The fines imposed were subsequently not paid, often even through distraint proceedings.

9.1.3. Availability and enforceability of administrative sanctions.

The FIU SR may impose a fine on any obliged entity found to be in breach of its obligations under Act No. 297/2008 Coll. Act No. 297/2008 Coll. contains appropriate and dissuasive administrative sanctions applicable to individual companies. The Act allows the FIU SR, upon discovering that an obliged entity has failed to comply with its obligations for more than 12 consecutive months, to submit a suggestion to the competent authority for withdrawal of the authorisation. The lower scores for this variable were found mainly for the free trade licences: accountant, organisational and economic advisor, buying and selling, where it is possible to transfer the company to another person, even in the course of administrative proceedings, often to a foreigner, or insolvency at the time of execution, when the debt becomes unrecoverable (see previous variable 1.2.). In a petition for withdrawal of a licence in a free trade, the person is allowed to carry on business independently in several companies without any restriction, which implies that the sanction of "petition for withdrawal of licence" is ineffective in free trades. On the contrary, when evaluating professions such as lawyer, notary, auditor, court distrainor, tax advisor, this variable is very highly rated and in case of non-compliance with the obligation under Act No. 297/2008 Coll. may result in the loss of the licence, which the obliged entity will never obtain again. Administrative sanctions against employees and management cannot be applied by FIU SR. It is up to the obliged entity - the employer - to take corrective measures against the employee in case of violation of Act No. 297/2008. Consistent internal control and the application of appropriate corrective measures in relation to employees and managers in the event of non-compliance with their obligations under the Act is considered a very important obligation and, of course, a right on the part of the obliged entities.

9.1.4. Availability and enforceability of criminal sanctions.

This variable assesses not only the legal framework, but also the effectiveness and proportionality of criminal sanctions and measures applied to obliged entities, members of their management bodies and employees, in cases of non-compliance with obligations related to the prevention of money laundering and terrorist financing. All criminal sanctions are defined in Criminal Code No. 300/2005 Coll. and their enforceability by the Code of Criminal Procedure No. 301/2005 Coll., while since 1 July 2016 the criminal liability of legal persons has been introduced (Act No. 91/2016 Coll.).

In the period under assessment, there were no cases where criminal prosecution was initiated against obliged entities, members of their management bodies or employees in the event of serious violations related to non-compliance with the obligations arising from Act No. 297/2008 Coll. The general awareness of employees, especially in the case of free trades, is not adequate to the seriousness of the subject, which leads to the conclusion that the regime of criminal sanctions does not have a sufficient impact to positively influence the behaviour of individuals. For lawyers, notaries, court distrainors, auditors, tax advisors, where the difficulty of obtaining a licence is high, this awareness is at a sufficient level and criminal sanctions would result in suspension or, if proven guilty, even loss of the licence.

9.1.5. Availability and efficiency of input control mechanisms.

The conditions under which licences to operate in the non-financial sector can be obtained vary widely. The criteria for obtaining a licence are very strict for lawyers, notaries, auditors, tax advisors and court distrainors, where, in addition to a university degree, a condition is to pass a state examination, part of which is also focused on the prevention of money laundering and terrorist financing. If the licence is lost due to a serious violation of Act No. 297/2008 Coll., it is not possible to regain the licence. A specific group for licencing and control are gambling operators, where the licence was granted by the MF SR and since 1 June 2019, by the Gambling Regulatory Authority. The problem and downgrading of the mark on the assessment of this variable was identified by the working group in the granting of free trade licences for organisational and economic advisors and accountants. A very low rating for this variable was given to those with the subject of the activity accountant, who ensure the fulfilment of statutory levy obligations paradoxically without the need for adequate education and experience. Another group with a free trade licence is a legal or natural person who trades in precious metals and stones, who is allowed to carry out this activity only on the basis of a licence for the subject of the activity of buying and selling, provided that the entrepreneur registers in the register kept at the Assay Office of the Slovak Republic. The subject of mediation of sale, lease and purchase of real estate is a regulated trade, which can be operated on condition of acquisition of professional education and relevant experience. The postal undertaking (Slovenská pošta, a.s.), which performs universal postal services, is licenced by the Regulatory Authority for Electronic Communications and Postal Services. Other postal undertakings providing partial services are licenced by the Trade Licencing Office. For free trades, the age of 18 years and integrity is necessary. As it is a free trade, anyone can get it, without any experience and education. The problem with free trades is that once they are acquired, the owner can use them independently in several companies. Obliged entities with this subject of activity often do not even know that they are classified as obliged entities under Act No. 297/2008 Coll.

9.1.6. Integrity of business/profession workers.

All persons acting as lawyers, notaries, distrainors, tax advisers and auditors must prove their integrity. The problem of downgrading this variable is seen by the working group in the case of employees in free trades, where it is not necessary or not required by the employer to submit a criminal record and where there is the possibility of integrating employees who may be guilty of both negligent conduct and 'wilful blindness' in the exercise of their activity. Gambling operators require from their employees in the capacity of manager, croupier and from the employees dealing with funds an abstract of criminal records.

9.1.7. Knowledge of AML in business/profession.

AML issues are not given sufficient attention by the obliged entities, even if the obliged entity submits proof of compliance with the obligation to carry out training of employees for individual years during the inspection. Both the results of the inspections carried out by the FIU SR and the questionnaires sent by the respondents of the obliged entities revealed deficiencies in the exercise of customer due diligence, suggesting that the obliged entity does not know its customers sufficiently to be able to assess unusual transactions related to the employment and

status of the customers. Lawyers, notaries, auditors, distrainors and tax advisers consider the obligations arising from the various acts under which they practise their profession (e.g., the Act on Advocacy, the Notarial Code, etc.) to be sufficient to prevent the legalisation of proceeds of crime.

As the customer's funds do not pass through the account of the obliged entity, they do not consider it important to establish the origin of the funds or assets. These professions are aware of their obligations under the law, but the findings show that they take a superficial approach to their obligations and most often refer to the act under which they operate. Obliged entities classified based on free trade licences as accountants, organisational and economic advisors, entrepreneurs providing services to companies, in most cases do not even know that they are obliged entities, or do not know the legal obligations. The fulfilment of some obligations is often only formally ensured by the above-mentioned obliged entities after they have been sent an inspection notice by the FIU SR, or they do not allow the FIU SR to carry out an inspection.

9.1.8. Efficiency of the function for ensuring the compliance with requirements (of the organisation) – a person responsible for protection against legalisation.

In the non-financial sector, in particular in the professions of lawyer, notary, distrainor, auditor and tax advisor, the compliance function is usually performed by a person who has obtained a licence according to the profession practiced and who has the opportunity to assess the required business or business operation from the ML point of view already when obtaining a certain contract. As regards legal professions, they have a duty to refuse business on grounds of lack of confidence, which is also used by obliged entities. For regulated and free subjects of activity - this function is usually performed by the Executive Officer, who organises and manages the whole process from the identification of the UT, the assessment, to its reporting to the FIU SR.

9.1.9. Efficiency of unusual transaction monitoring and reporting.

Most of the non-financial sector has the possibility to follow a given transaction or legal or other act at the time of preparation and execution, which is a great advantage of the non-financial sector. The obliged entity is familiar with the facts. The legal or economic service is carried out on the basis of the documents submitted until it is completed. It is necessary to take into account the special provision on lawyers, notaries pursuant to Article 22 of Act No. 297/2008 Coll. and on auditors, accountants and tax advisors, pursuant to Article 23 of Act No. 297/2008 Coll., whereby they are not subject to the obligation to report an unusual transaction in the cases specified by law.

The low number of unusual transactions reported by obliged entities classified in the non-financial sector results from two main factors. The first fact is that, especially in the case of the free trades, there is still low awareness of the obligations arising from Act No. 297/2008 Coll. and the related understanding of the exposure to the risks of money laundering and terrorist financing. The second fact is the deliberate violation of the act, whether due to direct participation in illegal activities or due to the preference of business interests and profit over

the fulfilment of the reporting obligation within the meaning of the provision of Article 17 of Act No. 297/2008 Coll. (reporting unusual transactions to the financial intelligence unit).

9.1.10. Availability and access to information on beneficial ownership.

Until 14 March 2018, all obliged entities were obliged, depending on the risk of legalisation, to obtain information from the customer about the beneficial ownership, which the obliged entity was to verify in the written documents submitted by the customer. Since 15 March 2018 this obligation has been mandatory. The problem during the assessed period was the verification of information on beneficial ownership in companies based abroad.

9.1.11. Availability of reliable infrastructure of identification.

This variable assesses whether financial transparency and processes for customer identification and verification are of a high standard, and whether obliged entities in the non-financial sector are able to verify the identity of their customers using reliable and independent source documents, data or information. A good identification infrastructure should prevent the use of false documents and false identities. On the basis of the information and experience gained so far, it can be concluded that Slovakia currently has a very good and secure national identification system, as evidenced, for example, by the low number of intercepted false identification documents (hereinafter referred to as "IDs"). Each type of ID is regulated by a separate act and relevant regulations (ID Card Act, Travel Document Act, Asylum Act, etc.). Individual Slovak IDs are continuously supplemented with each new series by additional security features and signs, which complicate the possibility of their forgery. Obliged entities in the SR in connection with Slovak citizens' IDs have the possibility to use a verification service - a publicly accessible website of the MI SR aimed at searching for lost and stolen documents.

In its practice, the FIU SR has noted several cases where the obliged entity relied solely on the website of the MI SR - lost and stolen documents - in the process of identifying and verifying the identification of its customer. In this context, it should be noted that this is a database of previously issued ID cards and passports, whereas a false or altered document that has never been issued by a competent Slovak state authority cannot be found in the database of lost and stolen documents, which may represent a vulnerability for some obliged entities.

9.1.12. Availability of independent information sources.

This variable assesses the extent to which obliged entities have availability of and access to other independent and reliable sources of information within the basic customer due diligence processes. Based on the information available on this variable, it can be concluded that most obliged entities in the non-financial sector have access to the following independent information sources: Commercial Register, Trade Register, Internet and Address Register, Real Estate Register, and Register of Beneficial Owners. The distrainor, lawyer, notary have special access. Lack of accessibility due to time constraints was found for gambling operators (gambling venue, sale of lottery tickets) and precious metal dealers.

9.2.1. Lawyer

Obliged entity pursuant to Article 5 (1) (j) of Act No. 297/2008 Coll. is only a lawyer who provides legal services relating to any financial transaction or any other procedure which leads to or directly causes the movement of funds in:

1. purchase and sale of real estate or company or a part of them,
2. administration or safekeeping of financial resources, securities or other assets,
3. opening of an account in a bank or foreign bank branch or of a securities account and during their administration, or
4. establishment, activity or management of a business company, association of natural persons, association of legal persons, non-investment pooled asset fund or another legal person.

Summary of data obtained for the monitored period:

Year	2016	2017	2018	2019
Number of licences	5614	5762	5840	4341
Number of controls	0	0	0	0
Number of UTs	6	3	0	4
Sanctions	0	0	0	0

The assessed rate of overall vulnerability of lawyers is 0.42.

Strengths in observing AML:

- a state examination also containing the AML area,
- prescribed education,
- an overview of every legal service for which a detailed description of the facts is required from the customer, written supporting documents must be submitted,
- without mediators,
- Code of Ethics for Lawyers.

Weaknesses in observing AML:

- exposure to the risk of legalisation of proceeds of crime by the nature of their activities,
- insufficient legal regulation of lawyer's deposits (in contrast to e.g. the Czech Republic, which has a specific legal regulation concerning lawyer's deposits), the possibility of using only the general regulation of contracts of deposit provided for in the Civil Code,
- very poor compliance with the obligation to report unusual transactions to the financial intelligence unit,
- insufficient number of controls by the Financial Intelligence Unit.

In relation to the obliged entities - lawyers, the following threats of legalisation of proceeds of crime were identified:

- so-called lawyer's deposits, where two obliged entities act together: a lawyer and a bank, relying on each other to fulfil AML obligations; at the same time, in practice, banks often encounter reluctance on the part of lawyers to disclose information about

the owners of the deposited funds (depositors), under the pretext of the duty of confidentiality,
- transfers between the lawyer's deposit account and the lawyer's personal account,
- funds from abroad (especially from tax havens) are credited to the lawyer's deposit account,
- from the lawyer's deposit account, funds are withdrawn in large amounts in cash, or in smaller amounts, but often,
- cash deposits into the lawyer's deposit account by depositors,
- purchase of real estate, business shares on behalf of the customer,
- execution of cashless transfers on behalf of the customer, often to off-shore countries,
- establishment of business companies with non-transparent ownership structures,
- using the services of a lawyer to give the appearance of respectability/reliability.

9.2.2. Notary

Obliged entity pursuant to Article 5 (1) (j) of Act No. 297/2008 Coll. is only a notary who provides a legal service to a customer concerning any financial transaction or other action which is directed towards or directly causes the movement of funds in:

1. purchase and sale of real estate or company or a part of them,
2. administration or safekeeping of financial resources, securities or other assets,
3. opening of an account in a bank or foreign bank branch or of a securities account and during their administration, or
4. establishment, activity or management of a business company, association of natural persons, association of legal persons, non-investment pooled asset fund or another legal person.

A notary is a state-appointed person authorised to perform notarial activities pursuant to Act No. 323/1992 Coll. on notaries and notarial activities (Notary Code).

Overview of the data collected for the period under assessment:

Year	2016	2017	2018	2019
Number of licences	344	339	340	338
Number of controls	0	0	1	0
UT	1	0	4	0
Sanctions	0	0	15000	0

The assessed rate of overall vulnerability of notaries is 0.40.

Strengths in observing AML:
- a state examination also containing the AML area,
- prescribed education,
- the customer must submit written documentation for the requested legal service,
- without mediators,
- Code of Ethics for Notaries.

Weaknesses in observing AML include:

- failure to cooperate with the financial intelligence unit during inspections under the pretext of confidentiality,
- gaps in awareness of the potential risks of money laundering,
- insufficient customer due diligence (in particular failure to detect the origin of funds),
- almost no compliance with the obligation to report unusual transactions to the financial intelligence unit,
- insufficient number of controls by the Financial Intelligence Unit.

In relation to the obliged entities - notaries, the following threats of legalisation of proceeds of crime were identified:

- notarial safekeeping of money,
- frauds related to transfers of real estate, business shares and other rights, with the participation of a notary in the authentication of documents and signatures,
- using the services of a notary in order to legitimise old documents proving transactions that took place many years ago in circumstances that cannot otherwise be verified.
-

9.2.3. Court distrainor

The court distrainor is an obliged entity pursuant to Article 5 (1) (f) of Act No. 297/2008 Coll. only when selling real estate, movable property or a business and when receiving money, deeds and other movable things for safekeeping **in connection with the execution of the execution.**

The court distrainor carries out their activities according to Act No. 233/1995 Coll. on court distrainors and execution activities (the Execution Code) and on the amendment to certain acts. The Ministry of Justice keeps a list of court distrainors, notifies changes in the list of court distrainors to the Slovak Chamber of Distrainors and the courts, and exercises state supervision over the activities of the Slovak Chamber of Distrainors. The Ministry of Justice of the Slovak Republic appoints and removes distrainors.

Summary of data obtained for the monitored period:

Year	2016	2017	2018	2019
Number of licences	323	304	281	
Number of controls	0	0	0	0
Number of UTs	0	0	0	0
Sanctions	0	0	0	0

The assessed rate of overall vulnerability of distrainors is 0.28.

Strengths in observing AML:

- a state examination also containing the AML area,
- prescribed education,
- written documents used during the execution,
- Code of Ethics for Court Distrainors.

Weaknesses in observing AML include:

- insufficient efficiency of surveillance which is proved by the fact that for the monitored period, no control was performed,
- possibility to receive cash payments at auctions.

9.2.4. Tax advisor

Tax consultancy is a business, the subject of which is the provision of advisory services in matters of taxes, levies, fees and the provision of advisory services in matters of taxes according to special regulations. The status of tax advisors is regulated by Act No. 78/1992 Coll. on tax advisors and the Slovak Chamber of Tax Advisors. Tax advisors have compulsory membership of the Slovak Chamber of Tax Advisors. The Chamber issues licences to tax advisors, the supervisory authority is the Ministry of Finance of the Slovak Republic.

Overview of data on tax advisors obtained from the Slovak Chamber of Tax Advisors and the FIU SR:

Year	2016	2017	2018	2019
Number of licences	908	922	953	1120
Number of controls	0	0	0	0
Sanctions	0	0	0	0
Number of UTs	0	0	0	0

The assessed rate of overall vulnerability of tax advisors is 0.40.

Strengths in observing AML:

- a summary of the documentation on the transactions that are the subject of the tax advice,
- without mediators,
- without cash payments,
- long-standing business relationships and the resulting good knowledge of customers, enabling effective assessment of transactions in terms of their unusualness,
- Code of Ethics for Tax Advisors.

Weaknesses in observing AML:

- insufficient efficiency of surveillance which is proved by the fact that for the monitored period, no control was performed,
- the possibility of unwitting cooperation with perpetrators of tax crime,
- the use of highly specialised knowledge of tax law by perpetrators of tax crime.

9.2.5. Auditor

The auditor carries out their activities in accordance with Act No. 423/2015 Coll. on the statutory audit and on the amendment to Act No. 431/2002 Coll. on accounting as amended. The supervisory authority is the Audit Supervisory Authority. The Slovak Chamber of Auditors is an independent professional organisation which brings together auditors and audit firms registered in the relevant list. The list of statutory auditors and audit firms is maintained by the Audit Supervisory Authority.

Overview of data on auditors obtained from the Slovak Chamber of Auditors and FIU SR.

Year	2016	2017	2018	2019
Number of licences	1048	1042	1022	1020
Number of controls	0	0	0	0
Sanctions	0	0	0	0
Number of UTs	0	0	0	0

The assessed overall vulnerability rate of auditors is 0.39.

Strengths in observing AML:

- a state examination also containing the AML area,
- prescribed education,
- the customer must submit written supporting documents,
- without mediators,
- long-standing business relationships and the resulting good knowledge of clients, enabling effective assessment of transactions in terms of their unusualness,
- Code of Ethics for Auditors,
- procedure according to the International Standards on Auditing (ISA), where ISA 240 regulates the auditor's responsibilities relating to fraud in an audit of financial statements and ISA 250 regulates the auditor’s consideration of laws and regulations in an audit of financial statements,
- compulsory continuing education, which is monitored and evaluated annually and in a 3-year cycle separately; failure to meet the statutory number of hours is sanctioned,
- when performing an audit in a public interest entity, prior registration with the Audit Supervisory Authority is mandatory,
- review of audit performance quality in a 6-year cycle, to which each auditor is subject - carried out by the Chamber,
- quality review in a 3-year cycle in the performance of an audit in a public interest entity - carried out by the Audit Supervisory Authority,
- a special supervisory authority for the profession was established in 2008.

Weaknesses in observing AML:

- the possibility of misusing highly specialised knowledge of tax law to provide advice to persons wishing to commit tax crimes,
- there is no risk for the audited entities as this is prohibited by the Statutory Audit Act.

9.2.6. Gambling operator

During the period under assessment, the conditions for the operation and promotion of gambling games, the rights and obligations of gambling operators and gamblers, and the powers of authorising authorities and state supervision bodies were regulated by Act No. 171/2005 Coll. on gambling games and on the amendment to certain acts, and from 1 June 2019 by Act No. 30/2019 Coll. on gambling games and on the amendment to certain acts, as amended (hereinafter referred to as the "Act on Gambling Games").

Summary of data for the assessed period obtained from the FD SR, MF SR, FIU SR, Gambling Regulatory Authority.

Year	2016	2017	2018	2019
Number of licences	326	269	182	103
Number of inspections by the FIU SR	0	0	0	1
Sanctions of the FIU SR	0	0	0	0
Number of supervisions by the Gambling Regulatory Authority	* 43 309	* 21 921	*15 884	1891
Sanctions of the Gambling Regulatory Authority	1 x 3000	3 x 3000	5 x 3000	0
Number of UTs	15	2	106	14

*Total number of AML supervisions without breakdown.

The assessed rate of overall vulnerability of gambling operators is 0.43.
The detected legalisation risks connected with a particular type of product/activity:

9.2.6.1. Casinos

- insufficiently performed customer due diligence,
- in cases of politically exposed persons, not identifying the origin of the funds used to purchase the tokens,
- deficiencies in the monitoring of follow-up transactions,
- allowing persons from high-risk countries to gamble,
- of all gambling operators, casinos are the most aware of the risks of legalisation of proceeds of crime and are keen to put in place sophisticated systems to monitor customers and transactions.

9.2.6.2. Gambling on slot machines

- non-monitoring of successive operations,
- insufficiently performed customer due diligence,
- failure to assess higher cash deposits by the customer,
- the operation of gaming machines may be of interest to organised crime groups with the aim of legalising the proceeds of crime.

9.2.6.3. Lottery games

- low degree of attractiveness for the purpose of legalisation of proceeds of crime due to the low rate of return on the funds invested.

9.2.6.4. Betting games

- in betting games, there have been cases where players have deposited funds into their player accounts and withdrawn the funds from their player accounts after a certain period of time, without actually playing or playing only minimally,
- hedge betting - a player minimises the risk of loss by betting on both possible outcomes of the same event,
- in relation to betting operators, there was low awareness of the risks of legalisation of proceeds of crime, deficiencies in the monitoring of bets as well as of follow-up trades during the period under assessment.

9.2.6.5. On-line gambling games

- all of the above risks of legalisation of proceeds of crime also apply to online gambling, including the following additional risks:
- risks associated with the physical absence of the player - failure of on-line gambling operators to exercise enhanced customer due diligence,
- risks associated with the use of other risky products such as electronic money or virtual currencies, which present their own set of risks in terms of legalisation of proceeds of crime,
- a bet by a client which is deliberately lost in favour of another client, followed by an immediate transfer of the won funds to a bank account (money laundering without any loss),
- making payments by VISA, VISA Electron, MasterCard, Maestro, Diners Club payment cards, where the obliged entity cannot prove that the customer is acting on their own behalf.

Draft measures in the gambling sector:

1. elimination of cash payments,
2. use of player cards and player accounts,
3. an increase in the number of inspections by supervisory authorities,

4. using and also improving the monitoring systems to control customers/players and intercept follow-up trades.

9.2.7. Accountant

The accountant carries out their activities on the basis of a trade licence issued by the competent District Office, Department of Trades according to Act No. 431/2002 Coll. on accounting (hereinafter referred to as the "Accounting Act"). The subject of activity of the accountant, is a free trade, which implies that the accounting may today keep persons who meet the general conditions of trade operation. No training or experience in accounting is required, which can in many cases lead to unintentional errors and, consequently, to tax evasion.

Data on accountants provided by Departments of Trades and the FIU SR:

Year	2016	2017	2018	2019
Number of licences	84,773	115,448	122,341	103,938
Number of controls	0	2	0	1
Sanctions	0	7,000	0	10,000
Number of UTs	0	0	0	1

The assessed rate of overall vulnerability for obliged entities – accountants is 0.49.

Strengths in observing AML:

- obliged entities - accountants, by the nature of their activity, have at their disposal all accounting and other customer's documents necessary for the proper performance of their activity; it follows that they have a very good overview of business activities of their customers, which subsequently allows them to fulfil their obligations arising from Act No. 297/2008 Coll., i.e. to assess and subsequently compare the executed transactions of the customer with the forms of unusual transactions, which are regulated in their own activity programmes and in the event of detection of an unusual transaction to proceed pursuant to Article 17 of Act No. 297/2008 Coll. and report the unusual transaction to the FIU SR,
- performance of accountant's activities without an intermediary.

Weaknesses in observing AML:

- despite the above strengths that enable accountants to effectively detect unusual transactions, in the 2016-2019 assessment period, one case of an unusual transaction was reported by accountants to the financial intelligence unit; as a percentage, of the average number of persons authorised to keep accounts in the period under assessment, only 0.001% reported an unusual transaction,
- there are insufficient entry control mechanisms - free trade granted to anyone who applies for it, subject to the conditions of reaching the age of 18 and integrity without relevant economic education and experience, as confirmed by the number of entities authorised to carry out this activity,
- the ineffectiveness of supervision by the FIU SR,

- low knowledge of the issue of legalisation of proceeds of crime and the related obligations arising from Act No. 297/2008 Coll.

In relation to obliged entities - **accountants,** the following threats of legalisation of proceeds of crime were identified:

- the use of accounting methods to reduce clients' tax liability,
- the use of accounting methods to misrepresent the true value of a business company when it is transferred,
- unprofessional bookkeeping - no requirement for expertise.

9.2.8. Legal person or natural person authorised to carry out activities of organisational and economic advisor

A legal person or natural person authorised to carry out the activities of organisational and economic advisor performs its activities on the basis of a trade licence issued by the relevant District Office, Department of Trades according to Act No. 431/2002 Coll. on accounting. Within the framework of the trade licence for the activity of organisational and economic advisor it is possible to carry out **in particular** the following activities:

- advisory services in the preparation of projects for withdrawing funds from the EU for the EU Structural Funds (SF) and Cohesion Fund (CF),
- preparation of economic projects for withdrawing funds from the EU for the SF and CF,
- technical and organisational assistance in the implementation of projects for withdrawing funds from the EU for the SF and CF,
- marketing consulting,
- accounting consulting,
- media consulting,
- consultancy and development of security projects for the protection of personal data,
- consulting and development of security projects for entrepreneurs,
- consulting activities in the field of personality development, visage and colour,
- consultancy and certification in the field of management and quality systems,
- consultancy and certification of quality management systems for non-designated products,
- consultancy and certification of quality of services and persons,
- consultancy in the field of social behaviour,
- consultancy activities in the field of healthy lifestyle and healthy nutrition,
- personnel management consultancy,
- consultancy, training and coaching services in the field of human resources development.

As there are no strict rules for this subject of activity, what the entrepreneur can perform within the scope of the assigned licence, entrepreneurs also provide services for business companies, i.e., providing the registered office, registered office address, delivery address, receiving and forwarding of parcels and other related services for business companies. However, the above fact cannot be ascertained from the extract from the Commercial Register of the Slovak Republic, which consequently hampers the control activities carried out by the financial intelligence unit. The actual performance of activities of the obliged entity authorised to act as an organisational and economic advisor can thus only be ascertained during the actual

inspection of compliance with the obligations arising from Act No. 297/2008 Coll. by the financial intelligence unit.

Data on organisational and economic advisors provided by Departments of Trades and the FIU SR:

Year	2016	2017	2018	2019
Number of licences	209,804	280,571	304,693	292,327
Number of controls	2	2	5	3
Sanctions	20,300	7,000	15,500	15,000
Number of UTs	0	0	0	3

The data presented in the table show an increasing tendency in the violation of Act No. 297/2008 Coll. on the part of obliged entities authorised to carry out the activity of organisational and economic advisor. The overwhelming majority of violations are of Article 30 of Act No. 297/2008 Coll., i.e., failure of the obliged entity to provide assistance during an inspection. In the cases mentioned above, the companies in question were letter-box companies which do not accept correspondence and are purposively established to carry out a small number of non-cash transactions, but in large volumes, which often end up on foreign accounts of off-shore countries. Alternatively, these companies have been set up with no economic activity and subsequently transferred to natural or legal persons resident/based abroad.

The assessed rate of overall vulnerability of organisational and economic advisors is 0.58.

Weaknesses in observing AML:

- insufficient efficiency of supervision,
- availability and enforceability of sanctions,
- availability and enforceability of penal sanctions,
- failure to provide sufficient input control mechanisms - free trade, no education,
- the possibility of sophisticated assistance in the legalisation of proceeds of crime, especially in the establishment of companies on an unlimited scale, transferring to a large extent to foreigners, the provision of a registered office linked to the provision of services to business companies and accounting,
- ignorance of the AML Act.

9.2.9. Provider of services of asset management or services for business companies.

Act No. 455/1991 Coll. on trade licencing does not know the subject of activities of providers of services of asset management or services for business companies included among obliged entities pursuant to Article 5 (1) (k) of Act No. 297/2008 Coll.

These acts are carried out within the scope of the authorisations for:

- real estate lease connected with the provision of other than basic services related to lease,
- organisational and economic consulting,
- keeping accounts or
- administrative services.

Pursuant to Article 9 letter b) point 3. of Act No. 297/2008 Coll. it is an entrepreneur who provides any of the following services to third parties:

- establishment of business companies or other legal persons,
- acting as a statutory body, a member of a statutory body, a person who is under the direct management of a statutory body or a member thereof, a holder of procuration, the head of an organisational unit of a branch plant or other organisational unit of an enterprise, a liquidator of a business company or acting in a similar capacity in relation to third parties or arranging for such action by another person,
- the provision of a registered office, registered office address, address for delivery and other related services for legal persons and special-purpose pooled asset funds, irrespective of their legal personality, which administer and distribute funds,
- acting as the trustee of a pooled asset fund or arranging for such action by another person,
- cting as a proxy shareholder for a third party other than the issuer of securities admitted to trading on a regulated market which is subject to disclosure requirements under a special regulation, or arranging for such action by another person.

Due to the non-transparency of this subject of activity in the Trade Register of the Slovak Republic, it is not possible to quantify the number of entities providing any of these services.

Based on the evaluation of data and information obtained in relation to activities carried out by providers of asset management services or services to business companies, the risk of legalisation of proceeds of crime has been identified at a medium-high level-numerically 0.62.

The level of vulnerability was affected in particular by:

- low knowledge of AML/CFT issues,
- efficiency of AML/CFT control,
- low enforceability of sanctions,
- the possibility of establishing an unlimited number of companies, which are then transferred free of charge to other owners, who are then provided with services at a price that compensates for the change of ownership,
- non-transparent conduct of the activity (without a proper trade licence),
- carrying out this activity without a transparent object of activity (services for business companies are not a trade),
- insufficient overview of the number of entrepreneurs providing these services.

The possibility of establishing companies or other legal persons with a deliberately complex structure in order to hide the true identity of the beneficial owners has a negative impact on the risk level.

9.2.10. Postal undertaking.

The Regulatory Authority for Electronic Communications and Postal Services issues licences in the area of provision of postal services on the basis of Act No. 324/2011 Coll. on postal services and on the amendment to certain acts, and Act No. 402/2013 Coll. on the Regulatory Authority for Electronic Communications and Postal Services and on the Transport Authority and on the amendment to certain acts. The Regulatory Authority for Electronic Communications and Postal Services also keeps a register of postal undertakings, which is public and which also includes legal and natural persons which have other postal services in their scope of activity, including express delivery of parcels, etc.

Slovenská pošta, a.s. is the only postal undertaking that provides universal postal services.

Data on postal undertakings obtained from the Regulatory Authority for Electronic Communications and Postal Services and from the FIU SR:

Year	2016	2017	2018	2019
Number of licences	25	26	27	27
Number of controls	0	0	0	0
Sanctions	0	0	0	0
Number of UTs	22	3	2	1

In the case of transport, home delivery, distribution of advertising materials, freight forwarding, courier service, which are not postal services, it is sufficient to obtain only a licence from the Department of Trades of the competent District Office.

The assessed overall vulnerability rate of postal undertakings is 0.44.

Strengths in observing AML:

Taking into account the location of Slovenská pošta, a.s. branches – the possibility of using local knowledge.

Weaknesses in observing AML:

- the possibility of making cash payments,
- the variety of activities carried out,
- acting as an intermediary for other obliged entities,
- absence of AML/CFT controls,
- efficiency of the designated person's activities,
- low number of UT reports - recognition of UTs,
- insufficient training.

9.2.11 Legal person or natural person authorised to mediate the sale, lease and purchase of real estate.

Obliged entity pursuant to Article 5 (1) (i) of Act No. 297/2008 Coll. – trade licences are issued by the competent District Office, Department of Trades. This trade is a regulated

trade according to the Trade Licencing Act. In addition to integrity (an abstract of criminal records is required), education and experience are proved for this regulated trade.

Membership in the National Association of Real Estate Agencies of Slovakia or in the Union of Real Estate Agencies of Slovakia is voluntary.

Within their business activities, real estate agencies provide mediation of sale, purchase or lease of real estate. Real estate mediation is mainly about the combination of supply and demand, all other activities, e.g., ensuring the execution of contracts, assistance in cadastral proceedings, assistance with the arrangement of a mortgage loan, etc. are only supplementary services, which by virtue of the business licence are performed by other persons (lawyer, notary, financial intermediary). Every real estate agency, if it offers the preparation of contractual documentation as part of the commission, cooperates with a certain law firm or notary. In practice, it has been found that 99 % of transactions are financed to some extent (usually 100 %) by the mortgage loan, and customers' own resources are used to a minimum.

Overview of information obtained on legal persons and natural persons authorised to mediate the sale, lease and purchase of real estate.

Year	2016	2017	2018	2019
Number of licences	13,137	14,340	14,902	37,677
*	2952	3125	3426	2033
Number of controls	0	0	0	0
Sanctions	0	0	0	0
Number of UTs	0	0	0	0

* Number of tax entities who declared this activity as their main activity in their tax return.

The assessed level of overall vulnerability of legal and natural persons authorised to mediate the sale, purchase and lease of real estate is 0.47.

Strengths in observing AML:

- for each service, the obliged entity knows what the operation is and has the necessary information and written documentation.

Weaknesses in observing AML:

- ignorance of AML duties,
- availability and enforceability of penal sanctions,
- not paying attention to the value of the real estate from an AML perspective, as the funds do not pass through the real estate agency's account.

9.2.12. Legal person or natural person authorised to trade in precious metals or precious stones, to place on the market products made of precious metals or precious stones

Obliged entity pursuant to Article 5 (1) (m) of Act No. 297/2008 Coll. – trade licences are issued by the competent District Office, Department of Trades under the object of activity "purchase and sale of goods, wholesale, retail, trade in precious metals," etc. At the above

definition, Act No. 297/2008 Coll. refers to Act No. 94/2013 Coll. on hallmarking and testing of precious metals (Hallmarking Act) and on the amendment to certain acts (hereinafter referred to as the "Hallmarking Act"). However, the Hallmarking Act does not recognise the terms “legal person or natural person authorised to trade in precious metals or precious stones, and legal person or natural person authorised to place on the market products made of precious metals or precious stones”. The Hallmarking Act only imposes an obligation on those dealers who actually deal in precious metals and stones to register with the Assay Office of the Slovak Republic.

Indicators found in relation to legal person or natural person authorised to trade in precious metals or precious stones.

Year	2016	2017	2018	2019
Number of authorisations	*4560	*4655	*4749	*2096
Number of controls	0	0	0	1
Sanctions	0	0	0	20,000
Number of UTs	0	0	0	0

* Data from the register kept at the Assay Office of the Slovak Republic, in which entrepreneurs wishing to trade in precious metals are registered.

The assessed rate of overall vulnerability of dealers in precious metals and stones is 0.55.

The result of the assessment was **positively influenced by the limitation of cash payments** according to Act No. 394/2012 Coll. on limitation of cash payments, which **prohibits cash payments exceeding EUR 5,000** in the cases also related to the activities of dealers in precious metals or precious stones.

Weaknesses in observing AML:

- ignorance of the obligations arising from Act No. 297/2008 Coll.
- input control mechanisms - a free trade that can be obtained without education,
- non-transparency of the subject of activity in the Trade Register of the Slovak Republic or in the Commercial Register of the Slovak Republic (purchase and sale is sufficient),
- shortcomings in relation to staff training.

9.3. Evaluation of tasks from the previous NRA for the non-financial sector for 2011 to 2015.

The following tasks from the previous NRA were incorporated into the Action Plan to Combat Money Laundering and Terrorist Financing for 2019 to 2022.

Task No. 1 To ensure that obliged entities - gambling operators and obliged entities with the subject of activity accountant, organisational and economic advisor, dealer in precious metals and stones, pawnshop, legal person or natural person authorised to mediate the sale, lease and purchase of real estate were when applying for a licence notified that they are an obliged entity pursuant to Article 5 of Act No. 297/2008 Coll. and of their obligations under this Act.

In connection with this task, requests for the fulfilment of this task were addressed to the MI SR, the Department of Trades at the MF SR and later, after the establishment of the Authority, also to the Gambling Regulatory Authority.

Task fulfilment: According to the statement of the MI SR, General Government Section of the MI SR, Department of Trades, this task was imposed at a working meeting of the Departments of Trades held in the Podjavorník Mountain Hotel on 10 and 11 December 2018. In letter No. SVS-OZP-2020/016695 dated 12 June 2020, the MI SR, Department of Trades informed us that when trades are registered in person, the employees of individual Departments of Trades notify the business entities of the obligations arising from Act No. 297/2008 Coll.

According to information from all District Offices, Departments of Trades, in the past periods, there have been no decisions of business entities showing that they had desisted from registering a trade in the Trade Register of the Slovak Republic.

As a large part of trade registrations is made electronically, where there is no personal contact with the business entity, they are not notified of the obligations arising from Act No 297/2008 Coll.

The Gambling Regulatory Authority draws the attention of every person requesting a licence to the fact that they are an obliged entity within the meaning of Article 5 of Act No. 297/2008 Coll.

Task No. 2 To raise the obliged entities' awareness of the forms and methods of legalisation and of the obligations arising for obliged entities from Act No. 297/2008 Coll.

Task fulfilment: The FIU SR publishes guidelines on the website of the FIU SR, provides lectures on Act No. 297/2008 Coll. according to the demand of chambers and associations or individual obliged entities. According to the requests sent by obliged entities in the form of a qualified request, the FIU SR responds in writing to the questions asked in relation to Act No. 297/2008 Coll. and on the application of this Act in practice.

10. SECTOR OF OTHER FINANCIAL INSTITUTIONS

Module 6 – Vulnerability of other financial institutions (hereinafter referred to as the "OFI")

1st part: General information on the sector

The following liable entities belong to the **OFI** sector:

1. commodity exchange;
2. a financial agent or financial advisor (hereinafter referred to as **"Financial Agent"** and "**Financial Advisor**");
3. a legal entity or a natural entity authorised to carry out foreign exchange activities or cashless transactions with foreign exchange values or to provide foreign exchange monetary services (hereinafter referred to as the "**exchange bureaus**");
4. a legal entity or a natural entity authorised to trade the receivables (hereinafter referred to as the "**factoring**");
5. a legal entity or a natural entity authorised to conduct auctions outside executions (hereinafter referred to as the "**auctions**");
6. financial leasing or other financial activities according to a special regulation (hereinafter referred to as the "**leasing**");
7. payment institution, provider of payment services in a limited range, payment service agent and electronic money institution (hereinafter referred to as the "**PI, provider of payment services in a limited range, payment service agent and electronic money institution**");
8. a creditor.

According to the number of entities, the OFI sector in general can be said to be the one of the larger sectors. The country has a detailed overview of the number of liable persons (hereinafter referred to as the "Liable person"), as it grants the permits (registrations) for their activities in all OFI categories. The total number of entities that participated in National risk assessment II. is shown in Table 1. The overview of the number of liable persons in each category in 2019 is given in Table 2.

Table 1

Entities that participated in National risk assessment II.	NUMBER
Commodity exchange	1
Financial Agent, Financial Advisor	20
Exchange bureaus	15
Factoring	1*
Auctions	6
Leasing	1*
PI, Provider of Payment services in a limited range,	20**

Payment Service Agent, Electronic Money Institution	
Creditor	5
Total	69

*(entities approached through an association or chambers)

**(including the electronic money distributors)

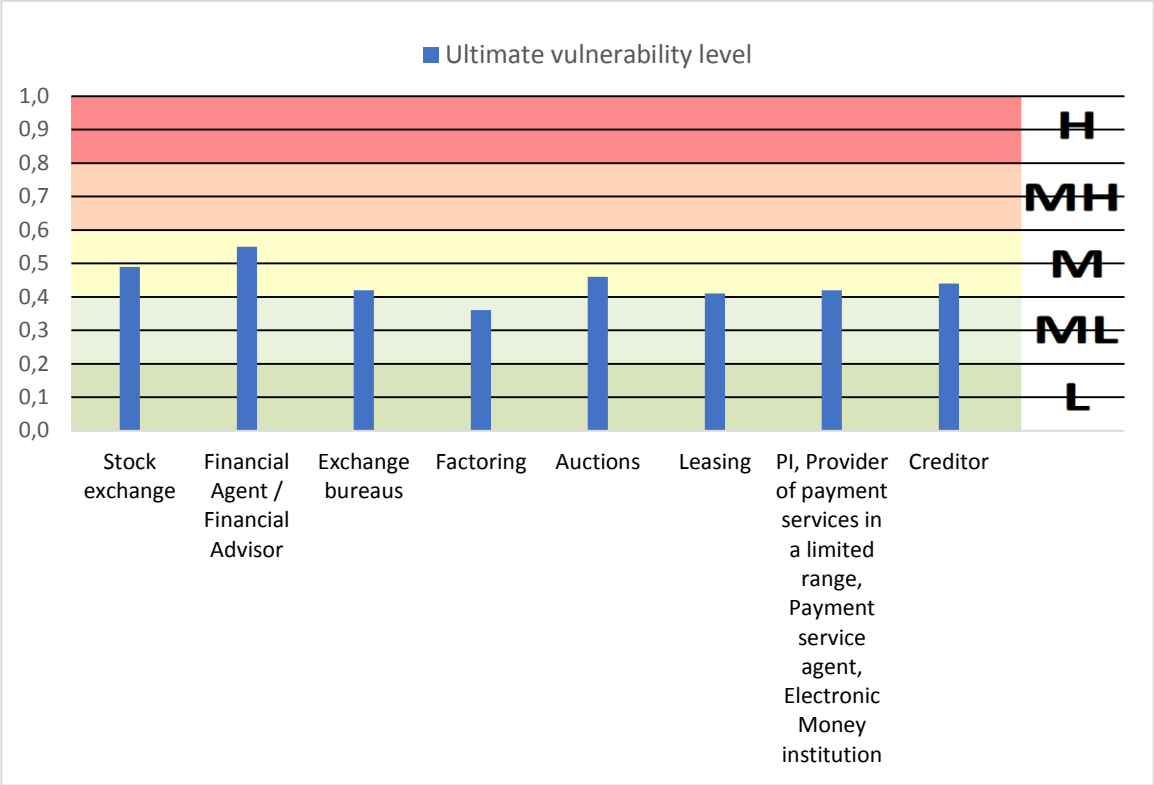
Table 2

Year/ Liable person	Stock exchange	Financial Agent, Financial Advisor	Exchange bureaus	Factoring	Auctions	Leasing	PI, Provider of Payment services in a limited range, Payment Service Agent, Electronic Money Institution	Creditor
2019	1	24319/ 12	1668	42601	701	34711	10/4/16/1	32

2nd part: Vulnerability level assessed

The ultimate vulnerability of the sector is on the border of medium and medium-low levels. At the medium level of vulnerability (M), the following categories were identified: financial agent, financial advisor (0.55), stock exchange (0.49), auctions (0.46), creditor (0.44), exchange bureaus (0.42), payment institutions, provider of payment services in a limited range, payment service agent, electronic money institution (0.42) and leasing (0.41). The last category factoring (0.36) reached the ultimate vulnerability level of medium-low (ML), see Chart 1.

Chart. 1 Ultimate vulnerability of individual OFI sector categories



The ultimate vulnerability of each category of the OFI sector depends on the *inherent vulnerability of each category of the OFI sector and quality and effectiveness of control mechanisms to combat money laundering/FT.* Inherent vulnerability is based on factors such as: overall size/volume of the category, category profile based on clients, usage of agents, level of cash payments, frequency of international transactions and other indicators of vulnerability. The quality and effectiveness of control mechanisms to combat the money laundering depends on the *quality of the policies and procedures to combat money laundering/FT* (e.g. effectiveness of supervision, availability and enforcement of the administrative sanctions) and *the quality of operations* (e.g. responsibilities and level of management control, level of staff compliance with requirements).

The number of inspections carried out by the Financial Intelligence Unit of the Presidium of the Police Force (hereinafter referred to as the "FIU SR") Control department of the liable persons in the OFI sector for the period assessed is shown in Table 3.

Table 3

Number of inspections carried out by the Inspection Department of Liable Persons for the period assessed													
		YEAR 2016			YEAR 2017			YEAR 2018			YEAR 2019		
		Number of inspections	Result of inspection	Sanction	Number of inspections	Result of inspection	Sanction	Number of inspections	Result of inspection	Sanction	Number of inspections	Result of inspection	Sanction
1.	COMMODITY EXCHANGE												
2.	FINANCIAL AGENTS	1		300									
	FINANCIAL ADVISOR												
3.	EXCHANGE BUREAUS				1		200				1		30000

4.	FACTORING				1								
5.	AUCTIONS	1		500			5000				1		500
6.	LEASING										1		5000
7.	PI												
	PROVIDER OF PAYMENT SERVICES IN A LIMITED RANGE												
	PAYMENT SERVICE AGENT							1		2000	2	a/a	300
	ELECTRONIC MONEY INSTITUTION												
8.	CREDITOR							1	a/a				

The number of inspections of NBS carried out is shown in Table 4. In the case of an independent financial agent and financial advisor, also to a natural entity entrepreneur.

Table 4

Number of AML/CFT inspections of NBS carried out on-site and remote									
Sector	Assessed period / number of on-site and remote inspections								Total
	2016		2017		2018		2019		
	on-site	remote	on-site	remote	on-site	remote	on-site	remote	
1. Financial Agent/Financial Advisor	0	540*	4	540*	2	0*	1	0	1087
2. Exchange bureaus	0	0	0	0	0	0	0	0	0
3. PI, Provider of payment services in a limited range, Payment service agent, Electronic money institution	3	0	2	0	1	0	0	0	6
4. Creditors	4	0	4	0	4	0	4	0	16
Total	7	540	10	540	7	0	5	0	1109

*Number of remote inspections on financial intermediation (in 2018 the AML questionnaire for 2016 and 2017 was sent to all entities)

3rd part: List of vulnerabilities

In the process of using the country risk assessment tool, we obtained an overview of vulnerability for each OFI category, showing the assigned assessments according to the assessment of the general input variables and the corresponding results of the assessment of the

intermediate variables which affect the fact, to which extent the assessed OFI categories are able to combat the ML/FT.

According to the above-mentioned process, the following common areas of weakness were identified for all OFI categories: availability and access to beneficial owner (hereinafter referred to as the "BO"), which has become more available in recent years but is still under-utilized. The average low level was the result for the availability and applicability of criminal sanctions, the availability of quality independent information sources and also for the overall effectiveness of the inspection. Subsequently, the values were obtained that indicate that the ability to combat ML/FT varies across categories at the same locations on different levels.

The following additional vulnerabilities were noted in each OFI category:

3.1. Stock exchange

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: quality of systems, quality of basic due diligence, quality of supervision, level of engagement and fulfilment of managerial responsibilities.

3.2. Financial agent, financial advisor

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: complexity of the legal framework to combat money laundering/FT, the effectiveness of supervision/surveillance, the integrity of the staff/institution, the knowledge of combat money laundering/FT of the persons doing business in the area/institution, the effectiveness of the compliance function with requirements and availability of the reliable identification infrastructure.

3.3. Exchange bureaus

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: the availability of the reliable identification infrastructure, the availability of independent information sources in the exercise of due diligence and the integrity of persons doing business in the area/institution.

3.4. Factoring

The quality and effectiveness of control mechanisms to combat money laundering/FT is low on average. The average level is represented by: quality of systems, level of engagement and fulfilment of managerial responsibilities, the effectiveness of monitoring and reporting the unusual transactions, quality of basic due diligence, the level of compliance of the staff of the institution, the effectiveness of compliance functions, input control mechanisms, quality and effectiveness of AML/CFT supervision.

3.5. Auctions

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: quality of systems, the effectiveness of the unusual transactions, level of engagement and fulfilment of managerial responsibilities, the level of compliance of the staff, the effectiveness of i.e. "compliance functions", quality of AML/CFT supervision, the effectiveness of supervision and control activities.

3.6. Leasing

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: do: the availability of the reliable identification infrastructure for carrying out the identification, integrity of the persons conducting the business in the area/institution, the availability of independent information sources for carrying out the diligence and the knowledge of the combat against money laundering/FT of the persons conducting business in the area of business/institution.

3.7. PI, provider of payment services in a limited range, payment service agent, electronic money institution

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: integrity of persons conducting business in the area/institution, knowledge of the combat of money laundering/FT of the persons conducting the business in the area/institution, the availability of the reliable infrastructure in conducting the identification, and the availability of the independent information sources in conducting diligence.

3.8. Creditor

The quality and effectiveness of control mechanisms to combat money laundering/FT is average. The average level is represented by: the knowledge of the combat money laundering/FT of persons conducting business in the area/institution, the effectiveness of the position of the AML/CFT officer and the compliance with the AML/CFT requirements imposed on him/her, the effectiveness of the established criteria in monitoring and reporting of suspicious activities.

4th part: Justification of vulnerability

4.1 Commodity exchange

The Commodity exchange organizes commodity trades pursuant to Act No. 92/2008 Coll. on commodity exchange and on the amendment of Act of the National Council of the Slovak Republic No. 145/1995 Coll. on administrative fees as amended (hereinafter referred to as the "Act No. 92/2008 Coll."). The country has one commodity exchange, which has about 20 direct members.

The permit to operate a commodity exchange shall be issued by the Ministry of Economy of the Slovak Republic upon fulfilment of the conditions laid down in Section 8 of

the Act No. 92/2008 Coll. The permit shall be issued for an indefinite period and shall not be transferrable.

Supervision of the activities of the commodity exchange shall be exercise by the state by means of the Stock Exchange Commissioner. The Act No. 92/2008 Coll. has been amended to ensure that the stock exchange operates in a safe and transparent regulated market for various commodities, excluding weapons and poisons. According to the research conducted, before a company becomes a member of the stock exchange, the chairman of the stock exchange personally attends a meeting with a representative of the company interested in becoming a member of the stock exchange. At the mentioned meeting, the basic due diligence will be performed in relation to the client pursuant to Act No. 297/2008 Coll. on protection against money laundering and terrorist financing and on the amendment to certain acts (hereinafter referred to as the "Act No. 297/2008 Coll.") and will subsequently decide whether the company will become a member of the Stock Exchange.

The trade with commodities takes place on a specially developed software which does not allow only authorized interventions. The trades are executed without the personal participation of the stock exchange members who trade by means of their brokers. Neither the seller nor the buyer knows the identity of the bidder on the other side; trading is anonymous until a certain stage of contractual execution. The trade is concluded when there is an agreement on the price on both sides, the so-called price matching under the same Incoterms terms and conditions. The system automatically generates a contract that is binding for both parties. The model contract and the execution of the terms and conditions are published on the stock exchange's website. The Buyer shall, three days prior to the collection of the goods, secure the funds for the purchase by cashless means to the credit of the account of the clearing house of the commodity exchange. The funds are released to the Seller's trusted account upon the delivery of the goods unless a claim process has been initiated. The trade is conducted exclusively in cashless form. The stock exchange does not accept cash payments or account deposits.

International payments are made, but their share is low as there are few non-resident member of the stock exchange. In real life, the trades on the stock exchange are mostly concluded by proven companies that have been dealing with the relevant commodity in their portfolio for a long time. The control of fulfilment and compliance with obligations of the provisions of Act No. 297/2008 Coll. shall be carried out by FIU SR. During the period under consideration, the FIU SR did not carry out any inspections and did not receive any unusual business operation (hereinafter referred to as the "UT") reports from the liable person.

The level of vulnerability in this category is likely to have been negatively influenced by factors such as the use of products without personal involvement. The brokers, after the initial verification of their identity, proof of representation of the member of the stock exchange (trader), execute transactions in the trading system contactlessly. The personal presence is only necessary when changing the broker and when negotiating a possible default on a contract.

4.2. Financial agent, financial advisor

The area of financial intermediation and financial advice is regulated by Act No. 186/2009 on financial intermediation and financial advisory services and amending certain laws (hereinafter referred to as the "Act No. 186/2009 Coll.").

A financial agent is a person who carries out financial intermediation on the basis of a written contract with a financial institution or on the basis of a written contract with an independent financial agent. Financial agent may not provide financial advice.

A financial advisor is a person who provides financial advice on the basis of a written contract for the provision of financial advice concluded with a client. The financial advisor cannot carry out financial intermediation.

Financial agents intermediate the financial products of financial institutions and financial advisors provide the financial advice in the sectors of:

- insurance and reinsurance
- capital market
- supplementary retirement savings
- acceptance of deposits
- lending and consumer lending
- old-age pension savings

The categories of financial agents pursuant to Act No. 186/2009 Coll.

Independent financial agent: carries out financial intermediation on the basis of a written contract with a financial institution and may have written contract concluded with several financial institutions at the same time.

Subordinate financial agent: carries out financial intermediation on the basis of a written contract with an independent financial agent. At the same time, a subordinate financial agent may have a written contract concluded with no more than one independent financial agent.

Tied financial agent: carries out financial intermediation on the basis of a written contract with a financial institution, while at the same time a tied financial agent may have a written contract concluded with no more than one financial institution, this does not apply to the insurance or reinsurance sector, in which a tied financial agent may have a written contract concluded with no more than one insurance company carrying out only life insurance and no more than one insurance company carrying out only life insurance at the same time.

Tied investment agent: is active in a capital market sector, it is a person who, under the full and unconditional responsibility of a security dealer, a bank authorized to provide investment services, investment activities and ancillary services, carries out financial intermediation for that person on the basis of a written contract.

Ancillary insurance intermediary: performs financial intermediation in the insurance and reinsurance sector as an ancillary activity, if the conditions laid down in Section 11 (c) of the Act No. 186/2009 Coll. are met.

The overall overview of the numbers of agents operating in individual sectors if the financial market (Insurance and Reinsurance, Capital Market, Acceptance of Deposits, Lending and Consumer Lending, Supplementary Retirement Savings, Old-age pension saving) for the assessed period 2016-2019 is shown in Table 5.

Table 5

Sector	Type of Agent	31 December 2016	31 December 2017	31 December 2018	31 December 2019
Insurance and Reinsurance	Independent Financial Agent	496	463	436	404
Insurance and Reinsurance	Financial Advisor	2	2	3	3
Insurance and Reinsurance	Tied Financial Agent	10,202	8,974	8,060	7,041
Insurance and Reinsurance	Subordinate Financial Agent	16,265	16,020	14,705	12,930
Insurance and Reinsurance	Ancillary insurance intermediary	-	-	4	4
Insurance and Reinsurance	Tied Investment Agent	-	-	-	-
Capital Market	Independent Financial Agent	125	122	111	106
Capital Market	Financial Advisor	1	1	1	1
Capital Market	Tied Financial Agent	499	494	405	397
Capital Market	Subordinate Financial Agent	5,590	6,473	7,248	6,907
Capital Market	Ancillary insurance intermediary	-	-	-	-
Capital Market	Tied Investment Agent	254	121	98	89
Acceptance of Deposits	Independent Financial Agent	137	130	123	112
Acceptance of Deposits	Financial Advisor	0	0	0	0
Acceptance of Deposits	Tied Financial Agent	2,172	1,889	1,518	1,365
Acceptance of Deposits	Subordinate Financial Agent	6,149	5,918	5,528	4,628
Acceptance of Deposits	Ancillary insurance intermediary	-	-	-	-

Acceptance of Deposits	Tied Investment Agent	-	-	-	-
Lending and Consumer Lending	Independent Financial Agent	245	235	218	202
Lending and Consumer Lending	Financial Advisor	8	9	10	10
Lending and Consumer Lending	Tied Financial Agent	4,964	3,637	2,996	2,610
Lending and Consumer Lending	Subordinate Financial Agent	8,893	9,200	9,115	8,783
Lending and Consumer Lending	Ancillary insurance intermediary	-	-	-	-
Lending and Consumer Lending	Tied Investment Agent	-	-	-	-
Supplementary Retirement Savings	Independent Financial Agent	80	76	74	71
Supplementary Retirement Savings	Financial Advisor	0	0	0	0
Supplementary Retirement Savings	Tied Financial Agent	951	1,008	992	981
Supplementary Retirement Savings	Subordinate Financial Agent	2,383	2,823	3,287	3,545
Supplementary Retirement Savings	Ancillary insurance intermediary	-	-	-	-
Supplementary Retirement Savings	Tied Investment Agent	-	-	-	-
Old-age pension saving	Independent Financial Agent	42	46	47	48
Old-age pension saving	Financial Advisor	0	0	0	0
Old-age pension saving	Tied Financial Agent	2,076	2,801	2,571	2,205
Old-age pension saving	Subordinate Financial Agent	4,402	4,904	5,306	5,452
Old-age pension saving	Ancillary insurance intermediary	-	-	-	-
Old-age pension saving	Tied Investment Agent	-	-	-	-
Total	Independent Financial Agent	585	554	519	479
Total	Financial Advisor	10	11	12	12
Total	Tied Financial Agent	14,127	12,017	10,657	9,239
Total	Subordinate Financial Agent	18,410	17,985	16,529	14,512

Total	Ancillary insurance intermediary	-	-	4	4
Total	Tied Investment Agent	254	121	98	89

Independent Financial Agent, Financial Advisor, Tied Financial Agent, Subordinate Financial Agent, Ancillary insurance intermediary, Tied Investment Agent

In 2019, a total of 24,319 agents were active in the area of financial intermediation, including **479 Independent Financial Agent** and **12 Financial Advisors.** The largest representation of agents is in the insurance and reinsurance sector.

On 15 March 2018, Act No. 52/2018 entered into force, amending and supplementing the Act No. 297/2008 Coll. Under the new legislation, the liable person under Section 5 (1) b) (6) is a financial agent, financial advisor, except for the performance of activities related to non-life insurance.

Pursuant to Act No. 297/2008 Coll., the inspection of the fulfilment and compliance of the obligations of the liable persons established by this Act is primarily performed by FIU SR. The National Bank of Slovak Republic shall also carry out the inspection the fulfilment and the compliance with the obligations laid down by the Act No. 297/2008 Coll. by the liable persons, **who are subject to supervision** of the National Bank of Slovakia pursuant to a special regulation.

The National Bank of Slovak Republic (hereinafter referred to as the "NBS") shall supervise pursuant to Act No. 747/2004 Coll. and pursuant to Act No. 186/2009 Coll. the performance of financial intermediation of the **independent financial agent** and the performance of the financial advisory services by a **financial advisor**.

The Act No. 186/2009 Coll. in the provisions of Section 29 imposes an obligation on financial institution and the independent financial agent to carry out the so-called delegated supervision over their subordinate entities consisting in continuous verification of compliance with the obligations under this Act, special regulations or other generally binding legal regulations that apply to the performance of the financial intermediation by subordinate entities. As part of its supervision, the NBS subsequently inspects whether the Independent Financial Agent and financial institution comply with these obligations under the Act No. 186/2009 Coll. Only independent financial agents are subject to direct supervision by the NBS, the number of which is generally lower compared to other categories of financial agents and financial advisors.

To carry out the activities of an independent financial agent and to carry out the activities of a financial advisor, the permission of the NBS is required. The NBS shall decide on the granting of a permit on the basis of an application. The conditions for granting a permit are laid down in Section 18 of the Act No. 186/2009 Coll. The permit may not be transferred to another person and shall not pass to a successor in title. The application for granting a permit of the applicant shall be accompanied by document demonstrating the technical and organizational

readiness to carry out financial intermediation or financial advisory, including the proposal of internal regulations and measures to prevent AML/CFT. At the same time, pursuant to Section 18 (11) and (12) of the Act No. 186/2009 Coll., the conditions for granting a permit, including the credibility of the applicant or the members of the statutory body, the supervisory body and the professional guarantor, must be fulfilled continuously during the entire period of validity of the permit to carry out the activity of the independent financial agent and the permit to carry out the activity of the financial advisor. The independent financial agent and the financial advisor are obliged to notify the NBS without undue delay of any changes in the facts that were proven when the permit was granted.

According to the organizational requirements for carrying out activities of financial intermediation and advisory, the Financial Agent and the Financial Advisor are required to regulate the relationship between the statutory body and the employees and the authority and responsibility of the Financial Agent and the Financial Advisor in the matters of protection of AML/CFT and to ensure, that persons responsible for carrying out the financial intermediation or financial advisory and the persons carrying out the financial intermediation or financial advisory are acquainted with the generally binding legal regulations and internal management acts that must be complied with in order to properly perform their duties and employ staff with the experience, knowledge and competence necessary to carry out their assigned tasks and activities.

The NBS conducted on-site supervisions at the Independent Financial Agent in the assessment period from 2016 to 2019, which included the AML/CFT area. The NBS identified the findings related to the failure of the professional guarantor to draft plans for supervising and monitoring of compliance with the obligations of the subordinate financial agents and employees performing the financial intermediation for the relevant calendar year, failure to verify the acquired knowledge from the professional trainings in the area of protection AML/CFT in the form of a test, and the program of own activities did not regulate the professional training of the subordinate financial agents. The NBS imposed recommendations on the entities to improve their activities for the above-mentioned findings. No sanctions have been imposed.

1. Questionnaire survey of the approached independent financial agents (hereinafter referred to as the “company”) and the analysis of the results

A. Integrity of the company’s employees

The companies require the submission of an extract from the criminal record not older than 3 months, a sworn statement that the person meets the conditions of integrity and trustworthiness. The companies stated that other documents they use to verify the integrity of the employees include references (for managerial positions), confirmation that there are no enforcement proceeding against the employee. Some companies do not verify the integrity of the employees on the grounds that they are one-person companies and do not hire new employees, or companies conduct financial intermediation through subordinate financial agents rather than through their own employees. During the period under consideration, there were 2 cases concerning a suspect of having committed an intentional offence of a pecuniary nature by

an employee and a breach of the condition of integrity. The companies immediately terminated the employment relationships with the employees.

B. Training of employees in the Financial Agent and Financial Advisory sector

The approached companies have training in the field of AML/CFT embedded in internal directives – Programs of their own activities. Training in knowledge of AML/CFT laws and procedures is conducted at the time of hiring the employees and then repeated on a regular annual basis thereafter. The overall level of knowledge of AML/CFT on the part of the employees (the obligation to report UT, the ability to assess the situations in which there is an increased risk of AML, understanding of the legal consequences in the event of a breach of the obligations arising from the Act No. 297/2008 Coll.) was most often rated by the companies with a score of 7 (from a numerical scale of 1- insufficient, 10 – excellent). Based on the questionnaires, it was evaluated that 10 companies conduct knowledge tests to verify the acquired knowledge in the field of AML/CFT of their employees.

C. Compliance system of the company

In the organisational structures of the companies, the function of the Compliance Manager provides assured independence. The statutory body – the company's board of directors and the professional guarantor placed under his/her authority is responsible for AML/CFT area. In smaller companies, due to the low number of employees, the AML/CFT area is the responsibility of the owner of the company. During the period under consideration, based on the questionnaires, a number of companies did not undergo an audit to assess the effectiveness of their AML/CFT legal regulations compliance.

D. Monitoring and reporting of UT

During the period under consideration, the companies used a manual AML/CFT monitoring system to identify the UTs and also a manual system to inspect new and existing clients for being on the sanction list or being politically exposed persons (PEP).

E. Availability and access to the beneficial ownership information

In the case of verification of the BO the use of information from the traditional sources such as the commercial register, the trade register, the register of public sector partners, from the websites www.minv.sk, www.mzv.sk, Finstat prevails. The approached companies have a questionnaire form in place (Record on Negotiation with Client, Record on requirements and needs of Client, Protocol on financial services intermediation). If the ownership structure is not clear and transparent after reviewing the standard documents, the companies require the necessary documents and information to be completed. In the event of non-submission, they will not enter into a contractual relationship with the client.

F. Identification and verification of client identification

During the period under consideration, the companies complied with the provisions of Acts No. 297/2008 Coll. and Act No. 186/2009 Coll. in the process of identification and identification verification of the client and in the process of identification and identification verification of the client – a natural entity, without his/her physical presence by means of technical means and procedures pursuant to the Act on AML/CFT. Before and in the process of using this technology, companies take into account risk factors in terms of product, business, distribution channel, geography, choice of external supplier and client risk assessment. Risk management in connection with the identification and identification verification of the client – a natural entity without physical presence shall be included in the Program of the entity's own activities and the use of the technical means shall be included in the content of the training schedule of employees who may come into contact with UT in the course of their work.

G. Sector profile based on clients

The AML risk assessment is always carried out by companies prior to the provision of a financial service, execution of a specific trade and during the duration of the business relationship. During the period under consideration, the entities performed basic and enhanced due diligence in relation to the client prior to the conclusion of the business relationship pursuant to Section 10 and Section 12 of the Act No. 297/2008 Coll., such as the identification of the client, identification of BO and the adoption of appropriate measures to verify his/her identification within the scope of the Section 31 of the Act NO. 186/2009 Coll. in conjunction with Sections 7 and 8 of the Act No. 297/2008 Coll. The companies shall ascertain whether the client is a PEP by means of a declaration in the client's application and contractual documents of the client and shall subsequently verify the information provided by the client in publicly accessible sources. Higher risk appears in companies providing financial services in the area of life insurance and investment, where the services were used by high-risk client from the AML/CFT perspective (companies most often reported PEPs). In those cases, the companies have exercised enhanced due diligence or have not provided the financial service to the client in question.

H. Level of cash activity

Based on the results of the questionnaire, the assessed companies do not accept cash, they make cashless transfers and payments with business partners/clients. The companies do not allow the acceptance of the cash in the intermediation of a financial service in their internal rules, thereby mitigating the risk of ML/FT.

I. Frequency of international transactions

The frequency of international transactions none or maximum up to 5% with countries Poland, Czech Republic, but the risk is low. In the FA and Financial Advisory sector, the entities do not use a system of foreign correspondent accounts. The vulnerability of the sector has been decreased as a result of the non-implementation of cash acceptance despite the fact that cash payments are allowed by law in this area and the low frequency of international transactions.

2. The effectiveness of AML/CFT supervision

The supervised entities are obliged to submit to the NBS at the end of each year, via the information system, a Statement on the performance of the financial intermediation and financial advisory. There is a separate section on AML/CFT compliance within the report, which contains a set of questions focusing on:

- Client risk – enhanced due diligence exercised towards the client.
- Product risk – use of cash transactions, volume of cash transactions.
- AML/CFT management, training, UT reporting.
- Control of compliance with the Program of own activities, identification of deficiencies and measures taken.

At the same time, the AML Questionnaire is sent to all supervised entities on a triennial basis through remote supervision, which focuses in detail on client risk, sector risk, product risk, distribution channels, AML management, trainings, transactions monitoring, UT reporting. Based on the results of the evaluation of the remote supervision, further remote or thematic on-site supervision shall be carried out in the event that facts come to light which make it necessary to carry out further inspection.

During the assessed period, no sanctions were imposed for breaches of legal regulations in the area of AML/CFT. The approached companies have developed a Program of own activities to comply with the obligations arising from the legal regulations aimed at the prevention of ML/FT. The companies have anchored the area of AML/CFT training of their employees in the Program of own activities. The trainings are mandatory for the employees.

3. Vulnerability of the FA and Financial Advisory sector

- Large number of entities in the market.
- Limited number of NBS employees for AML/CFT area.
- Low number of inspections by the FIU SR.
- Insufficient cooperation between the NBS and FIU SR, cooperation needs to be strengthened, especially from in terms of exchange of practical experience in the area of AML/CFT.
- The companies provide training of their employees at their own expenses. There is absence of training provided by another authority.
- Using of manual AML/CFT monitoring system to identify the UTs and manual systems to inspect new and existing clients for being on the sanctions list or being PEPs. As there is a large number of small entities in the sector, they do not use an automated monitoring system.
- Companies do not conduct audits to assess the effectiveness of organisational arrangement of AML/CFT legislation compliance.

4. AML/CFT threats in the FA and Financial Advisory sector

- Activity based exclusively on intermediation of products of other institutions (risk of insurance, credit fraud, risk of forgery and falsification of public documents, official seals).

- When intermediating a financial service, personal data is processed and may be misused for the financial enrichment of the perpetrator.

4.3. Exchange bureaus

1. Sector analysis

Execution of trades with foreign exchange values is regulated by the Act of the National Council of the Slovak Republic No. 202/1995 Coll. The Foreign Exchange Act and the Act amending Act of the Slovak National Council No. 372/1990 Coll. on offences, as amended (hereinafter referred to as the "Act No. 202/1995 Coll."). It is a regulated trade within the meaning of Act No. 455/1991 on Trade Licensing Act (Trade Licensing Act), as amended (hereinafter referred to as the "Act No. 455/1991 Coll."), which can be carried out on the basis of a trade licence, the obtaining of which requires the fulfilment of special conditions for the operation of the trade, i.e. the obtaining of a foreign exchange licence, which is issued by the NBS after the fulfilment of the conditions set out in the provisions of Section 6 of Act No.202/1995 Coll. The licence is issued for an indefinite period and is non-transferable. The conditions for termination of the licence are laid down in Section 24a of Act No. 202/1995 Coll.

The NBS records 1,668 entities that had or have been issued a licence to buy and sell foreign currency. Of these, there are 869 active and 799 inactive licenses. In the period under review for the years 2016 to 2019, the NBS issued 47 licences and 207 licences to operate exchange bureaus were terminated, see Table 6.

Table 6

Number of licences	Year				Total
	2016	2017	2018	2019	
Granted	11	9	12	15	47
Terminated	46	45	41	75	207

The NBS does not have information on the exact number of employees working at entities licensed to buy and sell foreign currency. From the results of the questionnaires sent by the exchange bureaus and processed for NRA II, we can conclude that most of the exchange bureaus have employees ranging from 1 to 3. Exchange bureaus are obliged to submit to the NBS data on executed transactions with foreign exchange values and data on their execution. This is data on the quantity of foreign currency cash bought and sold in the previous quarter.

The NBS has issued Measure No. 139/2013 Coll., which establishes details on the particulars of the application for a foreign exchange licence and details on the requirements for trading in foreign exchange. The exchange bureaus are subject to the supervision of the NBS. The employees of the NBS carry out supervision within the meaning of Section 24 of Act No. 202/1995 Coll. in conjunction with Section 29(3) to (5) of Act No. 297/2008 Coll. As part of its supervision, the NBS inspects compliance with the provisions related, inter alia, to keeping records of executed trades and data on clients, as well as the obligation to identify the client in the manner and within the scope of data provided for by Act No 297/2008 Coll. For each trade

with foreign exchange values, when carrying out foreign exchange activities, the foreign exchange office is obliged to identify the client in this way for each trade with foreign exchange values in the value exceeding EUR 1,000, unless Act No. 297/2008 Coll. stipulates otherwise. The NBS, upon detection of deficiencies in connection with non-compliance with the aforementioned provisions, may take a measure against the supervised entity to eliminate the detected deficiencies or impose a sanction.

2. Risk and vulnerability of the sector

Individual obligations in the area of prevention of ML/FT are primarily regulated by Act No. 297/2008 Coll. This law also regulates the obligation to apply a risk-oriented approach towards clients. Liable persons operating in the foreign exchange sector must have an overview of the potential risks associated with a particular client. On the basis of the information thus obtained, they are obliged to determine the scope of due diligence and, if necessary, to apply measures in the provision of enhanced due diligence. In the category of exchange bureaus, it is also necessary to prove the integrity of the employees working in the field of AML/CFT when submitting an application for a license, permit, trade licence. The entities did not record any breaches of the integrity of their employees during the period under consideration and there were no cases of suspected intentional offences of a pecuniary nature committed by the employees during the period under review.

3. Education

Most entities reported that employees' training is provided internally, within the entity's organization. This is mainly initial training and training on the recognition of counterfeit banknotes. AML/CFT training, including but not limited to UT Recognition, TF, Politically Exposed Persons (hereinafter referred to as the "PEP/PEPs"), BO are not included in the training structure for the employees of each entity. Moreover, the frequency of training is very low. For most entities, it is at the level of conducting one training session per year. Although Act No. 297/2008 Coll. imposes the obligation to carry out training of employees upon commencement of employment and once a year thereafter, the majority of entities assessed the knowledge of their employees as mediocre.

The absence of knowledge validation is also a negative phenomenon in the education of the employees of these entities. At the same time, it should be noted that training carried out by public authorities (FIU SR, NBS, etc.) is implemented only to a low extent. The level of understanding and mastery of AML/CFT issues can be determined by a numerical rating on a scale of 1 to 10 (where 1 is almost insufficient and 10 is excellent) at an average level of 6.

4. Organisational arrangement

The exchange bureaus sector consists mainly of small entities with one, two or three employees, but there are also entities that consist of several branches. The organizational arrangement of an AML-compliance system within the organizational structure of the institution, the system for determining the AML/CFT risk category of clients as well as the company's AML/CFT monitoring system for the detection of UT depend in the vast majority

on the subject of activity and the products offered. Larger entities in the survey reported that the AML compliance manager position in the institution's organizational structure has assured independence in decision-making. In most of the entities in the category of exchange bureaus, this activity is provided by a statutory representative, as they are companies with a small number of employees. The number of employees of the institution's specialised unit for the organisational, methodological and operational provision of ML/FT protection, involved in the provision of the ML/FT protection agenda, varies on average between 1 and 2 in larger entities. All of the companies interviewed in the survey reported that they had not experienced any breaches of legislation to ensure protection from ML/FT by their employees. A negligible percentage of entities use an automated AML/CFT monitoring system to check new and existing clients for being on the sanction list or the PEPs list. Many entities indicated in the questionnaire that they are able to provide this functionality with a manual system or that they are working on implementing an automated system. Subjects mainly use manual AML/CFT monitoring systems to detect UT according to established criteria. According to the survey, a low number of entities are conducting audits to assess the effectiveness of organizational arrangements and compliance with legislation in relation to measures to combat ML/FT. The number of UTs was in the range of 2-3 UTs for the period under review. One entity stated that it does not carry out UT monitoring as it is a "small" exchange bureau, thus violating the provisions of Act No. 297/2008 Coll.

5. Vulnerabilities in the foreign exchange sector

a) insufficient knowledge and awareness of ML/FT risks and their management

- deficiencies in employee training and in the validation of staff knowledge represent a significant vulnerability that has a direct impact on the performance of other exchange bureaus' activities. Although Act No. 297/2008 Coll. imposes the obligation to carry out training of employees upon commencement of employment and once a year thereafter, the majority of entities assessed the knowledge of their employees as mediocre. The absence of knowledge validation is also a negative phenomenon in the education of the employees of these entities.
- - clearly the most vulnerable point revealed by the evaluation process was the fact that not all exchange entities or individuals who inspect and manage these entities are aware that they are considered liable persons within the meaning of Act No. 297/2008 Coll.
- the insufficient and ineffective methodological and training activities carried out by the NBS can also be considered as a vulnerability in this area.

b) insufficient application of legislation

- strict compliance with Act No. 297/2008 Coll. and other generally binding legal regulations governing the status, roles and activities of entities in the exchange bureaus sector is an essential prerequisite for effective prevention. In the period under assessment, the NBS carried out a low overall number of supervisions in the foreign exchange sector. In the case of the NBS, there is a need to increase staff capacity in AML/CFT supervision. The lack of mutual cooperation, exchange of information and performance of joint inspections (supervisions) together with the FIU SR is also a vulnerability affecting the performance of supervision by the NBS. During the period

under consideration, there were no joint inspections of any of the entities active in the foreign exchange sector.

c) ineffective application of preventive measures in the AML/CFT area

- insufficient training and knowledge of employees as well as inconsistent compliance with AML/CFT legislation has a direct, but especially negative, impact on the performance of preventive measures by liable persons.
- the lack of methodological guidance for entities operating in the exchange bureaus sector on the fulfilment of obligations under legislation aimed at preventing ML/FT also has an increased potential for vulnerability. In particular, methods and forms of legalisation are noticeably absent.
- one of the effective tools, which, however, is largely absent in the case of exchange bureaus, is the regular performance of an audit aimed at assessing the effectiveness of the organisational compliance arrangements in relation to AML/CFT measures.

d) unusual business operations and transaction monitoring

- in particular, the fact that the vast majority of entities operating in the exchange sector use a manual AML/CFT monitoring system to identify UTs is a vulnerability from an organisational and technical point of view in terms of fulfilling their legal obligations, especially in relation to transaction monitoring and client monitoring and subsequent reporting of UTs. An equal proportion of these entities use manual systems to screen new and existing clients for being on the sanction list or being PEPs. A minimum number of exchange bureaus use automated monitoring systems.

4.4. Factoring

Factoring is a method of financing short-term credit extended for the supply of goods and services. The core of factoring is the purchase of short-term receivables without recourse (non-recourse) or with recourse (recourse) to the original creditor. Factoring is a form of financing that helps companies with cash flow problems due to deferred payments from their clients. The factor, i.e. the counterparty to a factoring trade, is most often the factoring company. The basis for the relationship is the factoring contract, which sets out the rights and obligations of both parties. Factoring is also commonly used in foreign trade.

Liable persons of this category carry out their activities in accordance with the provisions of Act No. 40/1964 Coll. of the Civil Code (hereinafter referred to as the "Civil Code"). It is a notifiable trade within the meaning of Act No. 455/1991 Coll., which can be carried out on the basis of a trade license, for which it is sufficient to reach the age of 18 years, have legal capacity and be able to prove the integrity of an extract from the criminal record. Supervision of compliance with the requirements in the fight against ML/FT in this category is carried out by the FIU SR. The number of entities that have this subject of business registered in their object of activity is on average around 41,000 and has an increasing tendency in the evaluated period. The country does not have an accurate figure on the number of entities actively engaged in this activity. Many entities have this activity registered as a business but do not actually carry out this activity. During the period under review, the FIU SR carried out 1 control and imposed 1 sanction in the amount of EUR 5,000. Tax crime is a higher risk than ML and TF when using this product. Most entities do not use cash payments or use them only

minimally. Representatives of this category in the survey assessed as insufficient that the activities of factoring companies are carried out according to the provisions of the Civil Code. The companies would adopt a separate law regulating the activities of factoring companies. When issuing the trade licence, the subject is not notified that in connection with the performance of this trade he/she is subject to the obligations of the liable person established by Act No. 297/2008 Coll. In the factoring category, the level of vulnerability was negatively affected mainly by the fact that many entities do not even know that they are liable persons.

4.4. Auctions

An auction or bidding is a sale in which an item is sold publicly at the same time to a larger number of bidders and the highest bidder receives the item sold. The term auction means a voluntary auction of a specific physical item at a specific location so that buyers can view or test the item. There are two basic methods of auction:

- English auction - the starting price is basic and the bid increases gradually,
- Dutch auction - if no one bids the starting price, the price is gradually reduced.

Online auctions are a special type of sale. This is a dynamically developing part of the market abroad. The price is not fixed and depends on supply and demand. In addition to new goods, it also includes used items, which can be sold through the auction system by anyone.

Advantages of online auctions:

- no time limits - bidding is possible at any point in time,
- no geographical restrictions - sellers and buyers can participate in auctions from any location with internet access,
- social interaction - the form of real-time bidding is fun and exciting from the perspective of the bidder,
- many bidders - bidding prices are lower than market prices and there is a wide range of products on offer on auction portals,
- many sellers - the large number of bidders and the element of competition often leads to higher final prices, minimal selling costs and easy accessibility.

The activities of auctioneers are regulated by Act No. 527/2002 Coll. on Voluntary Auction Sales, as amended, and on supplementing Act No. 323/1992 Coll. of the Slovak National Council on Notaries and Notarial Activities (Notarial Code), as amended (hereinafter referred to as "Act No. 527/2002 Coll."). It is a regulated trade within the meaning of Act No. 455/1991 Coll., the activity of which requires the fulfilment of special conditions for the operation of the trade set out in Section 6 of Act No. 527/2002 Coll., i.e. higher education and three years of experience, or secondary education and eight years of experience, as well as contracted contractual compulsory liability insurance. The Ministry of Justice of the Slovak Republic shall exercise control over compliance with the conditions for organising and conducting auctions. The FIU SR monitors compliance with the requirements to combat ML/FT in this category. During the period under review, the FIU SR carried out two inspections and imposed two penalties amounting to EUR 500.

The number of entities that have this activity registered in their scope of activity has decreased from 719 in 2016 to 701 in 2019. The country does not have an accurate figure on the number of entities carrying out this activity. Cash payment is also allowed for auctions. Auctions allow to deposit an auction security in cash, the value of which may not exceed 30% of the lowest bid but may not exceed the amount of EUR 49,790.88 (provided for in Section 14 of Act No. 527/2002 Coll.). The auction security shall be credited to the auctioneer in the price achieved by the auction. It follows from the provisions of Section 17 of Act No. 527/2002 Coll. that the price achieved by the auction may also be paid in cash. Auctioneers indicated in the survey that they see the risk of the ML/FT as precisely the possibility of accepting cash. The list of auctioneers is published on the website of the Ministry of Justice of the Slovak Republic, which in 2020 consists of 513 entities. The Notary Chamber of the Slovak Republic has been the administrator of the Notary Central Register since 2003, where the information specified by Act No. 527/2002 Coll. or information voluntarily provided by participants of auctions is publicly accessible. Act No. 527/2002 Coll. does not refer to Act No. 297/2008 Coll. In the auction category, the level of vulnerability was negatively affected mainly by the cash payment option.

4.5. Leasing

Leasing is the process by which a legal or natural person can acquire certain long-term assets for which they must pay a series of contractual, periodic and tax-deductible payments. The lessee is the recipient of the service or property under the lease and the lessor is the owner of the property. The relationship between the lessee and the lessor is called a lease and can be for a definite or indefinite period of time, called the lease period. Leasing is a form of business, the essence of which is the lease of products and means of production for a certain period of time. Similar principles apply to immovable property as to movable property, although the terminology may be different. The term of the lease may be fixed, periodic or indefinite.

Advantages of leasing:

- no capital required for a one-off payment,
- lease instalments may be identical to the actual performance parameters by agreement with the leasing company,
- saves finances.

Disadvantages of leasing:

- the service and profit of the leasing company is paid in instalments,
- limited ownership rights to the subject of the lease,
- termination of the lease agreement by the lessee with a high penalty.

Types of leasing:

- **Operational** – (short-term) where the lease term is shorter than the useful life of the leased item. The leased object is returned to the lessor at the end of the lease.
- **Financial** – (long-term) - the lease period is close to the useful life of the object. At the end of the lease period, the object remains with the lessee. Repairs and maintenance are the responsibility of the lessee.

Liable persons in this category shall operate in accordance with the provisions of the Civil Code. It is a notifiable trade within the meaning of Act No. 455/1991 Coll., which can be carried out on the basis of a trade license, to obtain which it is sufficient to reach the age of 18 years, to have legal capacity and to prove the integrity of an extract from the criminal record. The FIU SR supervises compliance with the requirements in the fight against ML/FT in this category. The FIU SR carried out 1 inspection in the reporting period, imposed 1 sanction in the amount of EUR 5,000. On average, the number of entities that have this line of business registered ranges from 33,458 in 2016 to 34,711 in 2019. The country does not have data on the exact number of entities carrying out this activity. Many entities have this activity registered as a business but do not carry it out. The use of cash in this category is allowed up to EUR 5,000. The interviewed entities stated in the survey that despite the fact that the law allows them to use cash, they use this option minimally or not at all. The majority of entities do not conduct international transactions; resident clients predominate. Even if international transactions are made, their share of international transactions is negligible compared to the total volume of payments.

In the leasing category, the level of vulnerability was negatively affected mainly by the fact that many entities do not even know that they are liable persons; we also perceive the implementation of cash payments as a negative.

4.6. Payment institution, limited payment service provider, payment service agent and electronic money institution

As of 31 December 2019, there were 10 payment institutions, 4 payment service providers in a limited scope, 1 electronic money institution, 16 payment service agents and 11 electronic money distributors operating on the Slovak financial market. We can state that the financial market for payment service providers is relatively new and overall developed although most of the entities were established between 2018 and 2019. The entities that participated in the NRS II for the period under review are listed in Table 7.

Table 7

Entities that participated in NRA II. / assessment period	2016	2017	2018	2019
Payment institutions	6	7	8	10
Payment service providers in a limited range	4	4	4	4
Electronic money institution	1	1	1	1
Payment service agents	1	1	2	2
* Electronic money distributors	1	1	1	3

* They were approached by NBS to participate in NRA II.

The payment institutions sector is characterised by the provision of payment services alongside other business activities (we do not observe a payment service provider that exclusively provides payment services). To a limited extent, **the sector of payment service providers** is currently exclusively represented by providers of electronic communication networks or electronic communication services.

In the case of payment institutions, payment service providers in a limited range, electronic money institutions, payment service agents and electronic money distributors, it can be stated that this sector has a mixed portfolio of clients (natural entities, natural entities - entrepreneurs, legal entities), however, **the portfolio of clients - natural entities prevails** in all assessed entities.

On the basis of the analysed information from payment service providers regarding clients, we register that the entities keep insufficient statistics (records) of clients, therefore it would be advisable for the entities to set up procedures for this area in order to achieve a more telling value of the data provided, which will be used for the purposes of the next national risk assessment.

Data for the purposes of NRA II, which were processed in the form of questionnaires as well as in the form of teleconference meetings, especially from the point of view of statistical data management, we assess as data with a weak telling value, therefore we recommend, in addition to the introduction of procedures for the purpose of more effective statistical management of these entities, to consider the amendment of Act No. 297/2008 Coll., so that (all) liable persons are obliged to provide correct, true and complete data and information for the purposes of the NRA. We also recommend that the NBS and FIU SR spread awareness of the importance of providing relevant data for NRA purposes and its impact on the overall AML/CFT risk assessment.

The principle of the provision of payment services remains essentially unchanged. The way in which payment services are provided is subject to major changes and is changing in line with the speed of financial innovation. Clients are using modern technology enabling remote communication, identification and authentication of their identity and new applications that allow them to use payment services quickly and securely from the comfort of their own home.

Payment institution, payment service agent and electronic money institution

The provision of payment services, issuance and administration of electronic money is regulated by Act No. 492/2009 Coll. on Payment Services and on Amendments and Additions to Certain Acts (hereinafter referred to as the "Act No. 492/2009 Coll."). The above-mentioned payment service providers and electronic money issuers are supervised by the NBS in the area of AML/CFT pursuant to Act No. 747/2004 Coll. and pursuant to Section 29(3) to (5) of Act No. 297/2008 Coll. Act No. 281/2017 Coll., which entered into force on 13 January 2018, transposed Directive 2015/2366/EU, also known as PSD2 Directive, into Act No. 492/2009 Coll., which introduced a change in terminology (changing the payment institution in a limited scope to a payment service provider in a limited range) and the extension of payment services to include a payment initiation service and a payment account information service (third parties).

A payment institution (Section 64 et seq. of Act No. 492/2009 Coll.) is a legal entity with its registered office and head office in the territory of the Slovak Republic, which is authorised by the NBS to provide payment services, and at least one payment service must be provided in the territory of the Slovak Republic in accordance with the authorisation granted. A payment institution authorised by another competent national authority in the European

Economic Area may also provide its services in Slovakia. Under this "European passport", an institution can conduct business either through a branch, an agent or on the basis of free cross-border provision of services.

A payment service agent is a natural or legal entity who, when providing payment services, acts on behalf of a payment institution.

As part of the authorisation procedure for granting a permit (registration) for the provision of payment services, the NBS assesses, among other relevant documents and information, the internal regulations governing management and internal control mechanisms, including risk management procedures, accounting procedures and internal regulations governing mechanisms aimed at the protection against the ML/FT. The provision of Section 69 of Act No. 492/2009 Coll. imposes an obligation on the payment institution to divide and regulate in the statutes the powers and responsibilities in the payment institution for the protection against the ML/FT. The provision of Section 70 of Act No. 492/2009 Coll. imposes an obligation on the payment institution to develop and maintain an effective internal control system. For the purposes of the Act, internal control means control of compliance with laws and other generally binding legal regulations, the statutes of the payment institution, the rules of prudential business conduct and protection against ML/FT.

An electronic money institution is a legal entity with its registered office in the territory of the Slovak Republic, which is authorised to issue electronic money, administer electronic money and carry out payment operations related to the issuance of electronic money. In addition to issuing and managing electronic money, it may carry out other business activities but cannot accept deposits. It is subject to the conditions and requirements under Act No. 492/2009 Coll. On the basis of a notification received by the NBS, it may operate throughout the European Economic Area. In addition, an electronic money institution may provide all types of payment services listed in its payment services authorisation, whereas a payment institution may only provide payment services and may not issue electronic money. Pursuant to Section 81(10) of Act No. 492/2009 Coll., an electronic money institution **may offer and exchange electronic money through other persons (distributors)** acting on its behalf and on the basis of a written contract. The position of electronic money distributors is similar to that of payment service agents. Pursuant to Section 82(4)(g) of Act No. 492/2009 Coll., in the framework of the authorisation procedure, the NBS shall, among other relevant documents and information, assess the internal regulations governing the management and internal control mechanisms, including risk management procedures, accounting procedures and internal regulations governing the mechanisms aimed at the protection against the ML/FT, in the case of an **authorisation for the issuance and management of electronic money**.

The NBS website **publishes a list of financial market entities** that have been granted a permit to operate. For an overview of the NBS human resources for the supervisory area for the provision of payment services and the issuance and management of electronic money and for the AML/CFT area, see Table 8.

Table 8

Overview of human resources of the NBS in the area of supervision for the area of provision of payment services and issuance and management of electronic money and for the area of AML/CFT		
Assessed period	Number of supervisory employees for the area of payment services and electronic money issuance and management	Number of AML/CFT employees
Year 2017	5	2
Year 2018	4	3
Year 2019	5	1

In the assessment period from 2016 to 2019, the NBS carried out 6 on-site supervisions. In **2016**, a combined on-site supervision was carried out in three companies, where, among other things, violations of Act No. 492/2009 Coll. and violations of internal regulations in the area of AML/CFT were identified. In **2017**, a combined on-site supervision was carried out in two companies, where violations of Act No. 747/2004 Coll., Act No. 492/2009 Coll. and violations of internal regulations in the area of AML/CFT were identified, among others. In **2018**, a combined on-site supervision was carried out in one company, where, among other things, violations of Act No. 747/2004 Coll. and violations of internal regulations in the area of AML/CFT were identified. For the above findings from all 6 supervisions, taking into account the scope, severity and degree of repetition of the identified findings and the cooperation provided to the entity, the NBS **imposed measures to correct the deficiencies in the form of recommendations** to the entities. The overall vulnerability of the OFI sector in the Slovak Republic was determined to be at a **medium-low level** on the basis of an assessment of aggregated information and data.

After a comprehensive assessment of the entities involved, we perceive that the sector of payment services and electronic money institutions is more vulnerable compared to the first ALM/CFT risk assessment, its vulnerability increases in direct proportion to the use of new technologies, to the coverage of new clients who are not clients of another payment service provider, i.e. banks, as well as to the efforts to cover with services the financial market that is not yet covered. In the area of payment services, we have recently seen an increase in interest from the perspective of companies (start-ups, fintech and IT companies) that intend to provide technical support in the provision of payment services or bring innovative solutions for the provision of payment services.

PROCESS VULNERABILITY OF THE SECTOR:

In terms of evaluating the procedural aspect related to the performance of activities and internal processes of individual entities of the sector, as well as supervisory and inspection bodies, it can be stated that a negative impact on the overall level of vulnerability and the most deficiencies were identified in the following areas:

4.7.1. The complexity of the legal framework in the fight against ML/FT

The legislative framework for the provision of payment services consists of:

1) Act No. **297/2008 Coll.** on the Protection against the money laundering and terrorist financing and on the Amendment and Supplementation of Certain Acts in Section 5(b)(14), according to which a payment institution, a payment service provider in a limited range, a payment service agent and an electronic money institution are considered to be a liable person. A selected sample of electronic money distributors was also included in the second national risk assessment. However, the Slovak Republic continuously monitors this sector.

2) other laws, regulations, guidelines with lesser or equivalent legal force in that area, e.g.:

- ✓ Directive 2018/843/EU of the European Parliament and of the Council (5AMLD) and Directive 2015/2366/EU (PSD2),
- ✓ Act No. 492/2009 on payment services,
- ✓ Act No. 483/2001 on banks (partially),
- ✓ Act No. 315/2016 on register of public sector partners,
- ✓ Regulation 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds
- ✓ NBS Methodological Guideline No. 4/2019 on the protection of PIs, Payment Service Agents and Electronic money institutions against the ML/FT,
- ✓ Act No. 289/2016 in implementation of international sanctions,
- ✓ MONEYVAL 2020 Evaluation Report,
- ✓ FATF Standards 40,
- ✓ FATF documents on the risk-based approach (RBA),
- ✓ Methodological guidance on the statutory provisions of the provisions (Act No. 297/2008 Coll.),
- ✓ Act No. 101/2010 Coll. On Demonstrating of the Origin of Property,
- ✓ Act No. 300/2005 (Criminal Code),
- ✓ Act No. 91/2016 (criminal liability of legal entities),
- ✓ Act No. 394/2012 Coll. on Restrictions on Cash Payments,
- ✓ Act No. 747/2004 Coll. on financial market supervision,
- ✓ Cooperation agreement between the NBS and the FIU SR,
- ✓ EBA (European Banking Authority) opinions, recommendations and guidelines),
- ✓ Opinion No. 1/2018 on the identification and verification of the identification of a client - a natural entity, without his/her physical presence, by means of technical means and procedures pursuant to the Act on the Protection against ML/FT,
- ✓ NBS website on AML/CFT for payment services and electronic money, etc.

In general, we can conclude that the legislative framework for the area of payment services and issuance of electronic money is in place, but what is **largely absent in practice is the practical application of the individual provisions of Act No. 297/2008 Coll. for the sector of payment services and electronic money institutions.** A possibility to improve this practical application is the issuance of joint FIU SR and NBS opinions (e.g. issuance of an opinion including a set of questions and answers on the AML/CFT area).

4.7.2. Effectiveness of supervision/control procedures and methods

The AML/CFT area is subject to a dual control (supervision) mechanism. The exercise of control over all liable persons pursuant to Section 5 of Act No. 298/2007 Coll. is primarily carried out by the FIU SR. Supervision of liable persons representing the financial sector with authorisation or registration is carried out by the NBS. On-site and remote supervision is primarily carried out by the NBS pursuant to Act No. 747/2004 Coll. and internal related procedures. Education and open communication of the NBS with payment institutions, payment service providers in a limited range, electronic money institutions, payment service agents as well as electronic money distributors is an integral part of on-site and remote supervision. **Taking into account the limited number of NBS employees for AML/CFT, a low number of on-site and remote AML/CFT supervisions are carried out. The limited number of both NBS and FIU SR employees has an analogous impact on the quality, frequency and effectiveness of supervision.** There is a need to increase the focus on AML/CFT in relation to payment service agents by exercising supervision. It is necessary to strengthen the cooperation between the NBS and the FIU SR in terms of sharing practical experience in the field of AML/CFT not only at the level of the management of these authorities, but also at the level of the employees who actually carry out supervision. **The area of cooperation between the NBS, the FIU SR and other supervisory authorities within the European Union also needs to be strengthened in the context of licensing procedures,** e.g. when verifying the trustworthiness of persons who intend to manage a company to be licensed or registered.

4.7.3. Existence and enforcement of administrative sanctions

In the area of AML/CFT, a diverse range of sanctions are not applied in relation to payment institutions, payment service providers in a limited range, electronic money institutions and payment service agents; **the predominant application of measures is of a recommendatory nature.** This recommendation element of the measures results in entities not being motivated to upgrade their AML/CFT measures and practices. On the contrary, the imposition of corrective measures in the form of recommendations encourages entities to repeat AML/CFT violations. On the other hand, corrective measures are imposed on entities at a low frequency, which is a consequence of the limited (low) number of NBS supervisory staff in the AML/CFT area. **The NBS employees supervising AML/CFT lack many years of practical experience** on how to supervise this area and what to focus on, which is partly due to their frequent turnover as well as the lack of time for its implementation.

4.7.4. Knowledge of AML/CFT combat of corporate/institutional employees

Pursuant to Section 20(1)(j) in conjunction with Section 5 of Act No. 298/2007 Coll., payment institutions, payment service providers in a limited range, electronic money institutions are obliged to regulate the timetable and content of the training of their employees in the Programme of own activities. **These entities mostly provide their own training, only occasionally training is provided by another authority.** The assessment of the AML/CFT training area showed that there is interest in training from another authority. However, there is little quality AML/CFT training provided in the Slovak Republic. Improvements in this area could be reinforced by training by the NBS and the FIU SR, or by another educational authority. Training of employees is carried out on an "automated basis" i.e. it is largely done only formally

with a lack of a limited number of repetitions of carrying out such training. The assessment of the NRA II entities revealed that in practice there is very little consultation/discussion with the NBS/FIU SR in the area of AML/CFT.

4.7.5. Effectiveness of monitoring and reporting of unusual business operations

One of the fundamental pillars that forms part of the monitoring systems is the monitoring and reporting of UTs. The monitoring systems targeting UT are dominated by manual monitoring systems with combined automated monitoring systems. In 2019, we have seen a trend of entities where, over time, they intend to move to an automated UT monitoring system. The assessment carried out on the reporting of UTs by FIU SR entities showed that the reporting of UTs by FIU SR entities is minimal. This may be due to the fact that the entities have inadequately set criteria for monitoring UTs or UTs occur at a low level in the entities. We **did not observe any UT associated with a payment services agent** in the reporting of UTs to FIU SR for all assessed entities.

4.7.6. Availability of and access to information on final ownership

In the case of BO by payment institutions, payment service providers in a limited range, electronic money institutions, the use of information from traditional public sources such as the commercial register, the trade licence register, the register of legal entities, the register of public sector partners and from the entities' own (internal) sources prevails. Neither entity reported using an established registry on BO. However, this register does not include all BOs. Payment institutions, payment service providers and, to a limited extent, electronic money institutions primarily verify BOs on the basis of KYC questionnaires and additionally verify end users from other sources. The NBS recognises that the absence of a single trusted source for verifying BOs is a major negative for these entities, making their process of verifying BOs substantially more difficult in practice and resulting in varying indicative value. Some entities did not report information or reported a zero count for BOs who were denied a business relationship, indicating that they have a relatively credible sample of clients.

4.7.7. Availability of independent information sources

PIs and electronic money institutions make relatively good use of their resources, which they do not, however, update on a regular basis. During the assessment period, we have seen an upward trend in the number of data updates used by entities to update their clients in more detail. We did not observe cooperation between these entities in terms of information sharing, which may be primarily influenced by the fact that these entities perceive each other as competing institutions with similar ways of operating in the financial market. The NBS perceives that the entities could be assisted by a common association, which would serve as a contact point for mutual sharing of information not only in the field of AML/CFT but also in other areas that would be useful in carrying out their activities.

- Conclusions from the NRA I. - implementation of the tasks of the Resolution of the Government of the Slovak Republic No. 207/2019, on the Action Plan, which summarizes the tasks from the NRA I. round

In our analysis of payment institutions, payment institution providers, electronic money institutions, we found that entities do not have much awareness of NRA I. The reason for this is that a small sample of the entities assessed participated in NRA I. The insights from NRA I were mainly demonstrated by those entities who participated in it, here we see the rationale for conducting the NRA analysis on a broader sample of entities. Many entities were not aware of the NRA I but expressed interest in collaborating on it. If there were continuity of assessment for the assessed entities under NRA, it would be possible to monitor and compare the evolving AML/CFT trend, and at the same time the entities could improve the setup of their information sources more closely.

- Summary information on payment institutions, payment service agents and electronic money institutions under NRA II for the assessment period 2016 to 2019

A. Organization of AML - a compliance system in the company

AML/CFT monitoring and data collection systems

Payment institutions:

- in 2016-2017, two payment institutions did not have a person responsible for the operational and methodological area of AML/CFT,
- most entities have a manual monitoring system (larger payment institutions that have been in the financial market longer have an automated system),
- The NBS identified the need to set criteria in the monitoring systems and create scenarios that would be applicable to the business model (payment service provided),
- The NBS identified that payment institutions do not pay sufficient attention to low-value trades and do not take into account the risk of chaining of such trades, the UT mechanism should be balanced,
- The NBS has identified the need to adjust the frequency within monitoring systems (transactional monitoring).

Payment service agents:

- The organisation is covered by payment institutions in the Slovak republic or cross-border payment institution.

Electronic money institution:

- conflict of interest within the competence of the AML/CFT officer.

B. Integrity of employees

Payment institutions:

- four payment institutions verified integrity from only one source (criminal record extract only)
- no payment institution has recorded a sanction against its employees for breach of trust

Payment services agents:

- have only one source of integrity verification

Electronic money institution:

- NBS recommends introducing an additional source for credibility verification and incorporating it into its own programme of work (not using multiple sources)

C. Availability of and access to information on a PEP

Payment institution:

- verify PEPs, verify the ownership structure, but rely only on statements from PEPs, only one payment institution also verifies PEPs from other available sources

Payment services agents:

- PEPs are required to declare and create their own databases for the purpose of a good data base, as purchased databases are not trustworthy
- the actual verification of the PEPs declarations is done by the parent company

Electronic money institution:

- provides PEPs with a KYC questionnaire and when a person is a PEP they require a separate declaration on the origin of assets of the PEP and close persons
- new PEPs and close persons verify within their own system

D. Availability of and access to client identification verification information

Payment institutions:

- five payment institutions do not perform customer authentication without physical presence
- three payment institutions perform customer authentication without physical presence with a technical means

Payment services agents:

- do not remotely identify the client without being physically present

Electronic money institution:

- does not remotely identify the client without being physically present

E. Risk-oriented approach

Payment institutions:

- five entities out of 10 do not have a properly developed RBA and incorporated into their own work programme
- two entities out of 10 have no RBA at all
- six entities out of 10 do not have a risk-oriented matrix for assigning their entities to risk groups in accordance with Methodological Guidance of NBS No. 4/2019

Payment services agents:

have RBAs that their parent companies cover

Electronic money institution:

- although they have RBA, this setting is not in accordance with Methodological Guidance No. 4/2019, they do not monitor the riskiness of the client and their setting is not sufficient

F. Measures against terrorist financing

Payment institutions:

In general, it can be concluded that entities do not pay sufficient attention to FT. Terrorist financing is done by entities on a formal basis. While entities monitor persons on sanctions lists, they do not have a set frequency for monitoring the business relationship. For the area of international sanctions, the entities did not have specific procedures in place. There is no monitoring of the business relationship of existing clients (they monitor their clients at the beginning of the business relationship, but then do not monitor these clients or have a long monitoring period). Transactional monitoring of clients against the sanctions list is done sufficiently by all entities, however, this monitoring is not done on a frequent basis

Payment services agents:

The monitoring of the business relationship is fine, it is done by their parent company. They plan to expand their systems in relation to new clients and sanctions lists. DEP should increase its emphasis on monitoring the business relationship with existing clients. Payment service agents should strengthen the monitoring of clients in relation to the sanctions list (monitoring is not done online but ex post).

Electronic money institution:

There is no monitoring of the business relationship of existing clients (they monitor their clients at the beginning of the business relationship, but then do not monitor these clients or have a long monitoring period). Transactional monitoring of clients against the sanctions list is done relatively well by the electronic money institution, but this monitoring is not done with sufficient frequency.

Payment institutions, payment services agents and electronic money institution

Three entities out of the 20 have clients that trade virtual currencies in terms of the 2016 to 2019 assessment period. These clients are trending downwards for the entities. The NBS has advised entities (that have clients that trade in virtual currencies) to develop a virtual asset process in line with INR. 15 (FATF). If entities do not have such clients, they should include virtual currencies, for example, as a non-supported activity in Program of their own activities.

4.8. Creditor

The provision of non-bank loans is carried out from the companies' own resources, the legal acquisition of which is always verified by the NBS during the licensing procedure for the granting of a licence to carry out the provision of loans. This category also includes leasing companies, whether established as subsidiaries of banks, automobile concerns, or companies focused on providing consumer loans for the purpose of purchasing selected consumer goods for clients. This also includes companies engaged in the purchase of bank receivables and their subsequent recovery from debtors. The supervised area of clients is represented by natural entities who are not entrepreneurs - consumers. When granting loans, the entities verify the client's income, verify identity almost always in the physical presence of the applicant, scan personal documents and verify them in the database of lost and stolen documents maintained by the Ministry of the Interior of the Slovak Republic, require payment when granting a loan to a bank account, and require repayment of the debt from the bank account. Cash payments are internally set by these entities as an unacceptable payment method. In view of the above, in their activities they understand that the ML/FT risk is primarily borne by banking entities in the management of individual client accounts, where it is possible for cash to be deposited into a particular account up to a limit amount by a person other than the account holder-contributor.

It can be stated that almost all consumer loans are granted to natural entities- residents, with permanent residence in the Slovak Republic, a very small part consists of persons - citizens of the Slovak Republic, temporarily living and working abroad (e.g. applying for leasing of

motor vehicles). The share of foreign nationals with permanent residence in Slovakia is not in the portfolios of the entities, but in terms of the number and volume of resources provided, it is nevertheless significant.

The ML/FT option is perceived for the purchase or lease of particularly more expensive motor vehicles or other means of transport/motorboats/yachts, their early repayment and subsequent possible sale. Here, the limiting factor is the threshold of EUR 75,000 of the funds provided falling within the definition of consumer credit. Any early repayment of a loan or lease is considered by companies to be disadvantageous, either because of impaired cash flow management or a reduction in interest income. Early repayment also involves contacting the client and requesting a justification for the early repayment, and many times, when the client is interested in a new contract again, refusing to finance it over a longer period of time.

The threat of FT is generally perceived as low, given the low social awareness or knowledge of the activities of terrorist groups in Slovakia. Recently, information about the activities of criminal business groups (not terrorists) has been leaked to the public through the media. These groups do not make use of consumer credit or consumer leasing as they are not dependent on these products.

Risk assessment within a supervised sector is only possible after a comprehensive on-site examination of the sector. The information collected from entities through remote supervision may not always correspond to the actual situation of the institutions concerned.

Therefore, the intention in forming supervision for the area was to develop a comprehensive overview of the performance of the entities based on on-site supervision, but this was hampered by the staffing of the supervisory team for the area of creditors. Initially, the strategy chosen was to examine the largest entities in terms of assets with the addition of one smaller entity. Later on, the surveillance plan was changed on an ad hoc basis, also on the basis of reported problems or complaints about the entity in question. The frequency of supervision was limited by the number of employees - 2 persons, which with simultaneous remote supervision - checking of reports and routine agenda allowed to carry out usually 4 supervisions per year

Product analysis:

In the case of creditors and their consumer clients, these are standardised types of transactions, e.g. car leasing, hire-purchase of consumer goods or short to medium term, mostly special purpose financial loans, loans as defined by the Consumer Credit Act. They are largely concluded with the participation of the client. Some companies conclude transactions without the participation of the client, e.g. one company provides online consumer loans without the participation of the client on its website, the condition is a bank account, permanent employment, documents - ID card or passport are scanned and sent to the company, mobile phone and access to internet banking. This service was introduced in 2019. Companies engaged in the purchase of banks' receivables and their subsequent recovery from debtors manage the purchased portfolio of receivables, trying to recover at least part of the debt from the debtors. Most of the time they don't provide new loans, they try to get the client to pay off old debts to other entities that they have taken into administration by buying them out. When the client's financial situation improves, they are able to restructure the client's debt.

Overview of the number: non-bank providers of loans without scope limitation - 32 entities, non-bank providers of loans with limited scope - 1 entity.

Creditor

A creditor is a person who offers or provides consumer credit. The activity is regulated by Act No. 129/2010 Coll. on consumer credits and other credits and loans for consumers and

on amendment and supplementation of certain acts, as amended (hereinafter referred to as the "Act No. 129/2010 Coll."). The creditor is supervised by the NBS. On 1 April 2015, an amendment to Act No. 129/2010 Coll. entered into force, which introduced a new authorisation procedure of the NBS for the provision of consumer loans in an unlimited or limited scope, or only for the provision of other credits and loans to consumers. Until then, providers of consumer credit and other loans could grant loans without authorisation until 31 August 2015 at the latest. The applicant for a permit to carry out the activity must demonstrate the conditions laid down in Section 20, Section 20a, Section 20b of Act No. 129/2010 Coll. In addition to other conditions, the applicant must prove his/her integrity with an extract from the criminal record, submit a programme of the liable person's own activity within the meaning of Act No. 297/2008 Coll. (not required for a creditor with a limited scope licence). The NBS has not recorded a case where an authorisation has not been granted due to non-compliance with the requirements of the control mechanisms in the fight against AML/FT. On 29 March 2016, the NBS issued the Methodological Guideline of the Financial Market Supervision Unit of the NBS No. 3/2016 on the submission of applications for authorisation to provide consumer credit and other loans and advances to consumers. Exercise of supervision and sanctions is regulated by the provisions of Section 23 of Act No. 129/2010 Coll., whereby this Act allows, pursuant to Section 23(3), to impose a monetary fine on a member of the creditor's statutory body, a member of the creditor's supervisory board, a proxy, the head of internal inspection for a violation of the obligations arising from Act No. 129/2010 Coll. or from Act No. 297/2008 Coll. An overview of the number of lenders (non-bank creditors) and on-site supervision by the NBS over the assessment period is provided in Table 9. The list is also published on the NBS website. During the period under review, the NBS carried out 16 on-site supervisory inspections and found no breaches of the requirements in the fight against AML/FT. No sanctions were imposed. The FIU SR carried out 1 inspection without sanction. The use of cash in this category is allowed in the case of early repayment of a consumer loan by a cash payment of up to EUR 5,000. The interviewed entities indicated in the survey that although the law allows them to use cash, they use this option minimally or not at all. Most entities do not execute international transactions; resident clients predominate. Even if they do, their ratio is insignificant compared to the total volume of payments. Pursuant to Act No. 129/2010 Coll., a creditor may use independent financial agents and tied financial agents for financial intermediation in the provision of consumer loans.

Table 9

Loan providers (non-bank creditors)		
YEAR	Number of entities	Number of on-site supervisions
2016	32	NBS 4
2017	34	NBS 4
2018	31	NBS 4
2019	32	NBS 4

The level of vulnerability in this category has been negatively affected in the past by factors:

- Provision of products through a high number of intermediaries - this vulnerability factor decreased significantly during the 2016-2019 assessment period compared to the previous NRA I assessment period;

- use of products without physical presence - the risk factor for products without physical presence has remained unchanged and the use of such products is likely to increase in the future;
- cash payment option - this vulnerability factor has decreased over the period under review, companies are moving away from this option.
  Risk factors

During the on-site inspections it was noted that the supervised entities did not update the Programme of own activities following the amended legislation. The entities were requested to update and submit the Programme of own activities in question. One such legislative change deals with the need to access sanctions lists maintained by the EU or the UN. However, given the presumed fact that their clients had already been vetted by banks when setting up and maintaining bank accounts, creditors were downplaying or omitting this obligation. These data were often difficult to trace for the entities in the past years, in the course of the supervisions carried out, the companies were instructed in case of unfamiliarity to external sources of information, later also to the website of the Ministry of Finance of the Slovak Republic, which has an internet section devoted to this issue with links to the individual databases.

Solution: on an ongoing basis during on-site supervisions, investigate the use of the required databases in the client verification process.

The second area of deficiency is the verification of PEPs. While the statutory provisions define the term PEPs, family members of a particular PEP also fall under the category of PEPs. Consistent compliance with the provision of the law in question requires that maintaining not a general but a nominal list of persons by the state administration, which would update this list on a regular basis, and this list would be made available free of charge to the liable persons-supervised entities. However, such a list may be in breach of the General Data Protection Regulation (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Solution: when conducting on-site supervision, consistently take into account the verification of PEPs and the checking of ongoing portfolio verification within a regularly set timeframe by supervised entities.

Cost savings in the provision of AML/CFT training can also be assessed as a risk factor. Companies in this sector typically use e-learning courses or external trainers. Better and more continuous training is of course provided by companies whose mother companies are part of international banking structures.

Solution: pay close attention to training activities when conducting on-site supervision.

Insufficient or inconsistently set internal inspection of the supervised entities themselves for the inspected AML/CFT area is also a risk factor. The on-site supervisions revealed that, in particular for entities that are not part of the bank's capital linked structures, internal inspections in this area are not carried out on a regular annual basis, or are highly formalised, or only a

certain area is reviewed cyclically for AML/CFT. When such findings were made in some entities, improvements were requested by the supervisory team in the area in question.

Solution: ensure that internal inspections in this area are submitted by supervised entities on an annual basis following on-site supervision.

The understaffing of the NBS supervisory team in the non-bank creditor sector can also be considered a risk factor. As the purpose of on-site supervisions is also to examine risks other than AML/CFT related to the activities of the supervised companies.

Solution: increase the number of staff for the supervised area of non-bank creditors.

There is also a risk in the lack of training for supervisory team employees for the subject area of non-bank creditors in the AML/CFT relationship, whether this is training within the NBS or from external training sources.

Solution: increase the offer and number of AML/CFT training courses in this area

4.9. Supervision, sanctions in the OFI sector

In the OFI sector, as mentioned above, in addition to the FIU SR, the NBS also has the authority to supervise the requirements in the fight against ML/FT and to impose sanctions for breaches of Act No. 297/2008 Coll. in the case of liable persons: financial agent, financial advisor, exchange bureaus, payment institution, payment services agent, electronic money institution and creditor. For other liable persons, only the FIU SR has a supervisory mandate. FIU SR, NBS may carry out remote and on-site supervision. The FIU SR does not carry out remote supervision, despite the fact that Act No. 297/2008 Coll. allows it to do so.

The NBS performs remote supervision in relation to the submission of statements and reports, for example, in the financial agent and financial adviser categories, which also include supervision of compliance with AML/FT requirements. On-site supervision shall be carried out according to a supervision plan taking into account the relevance of the supervised entity. The NBS also takes into account the requirements of the NBS expert departments, complaints or suggestions of clients or market participants. Pursuant to Section 29(5) of Act No. 297/2008 Coll., the FIU SR and the NBS may carry out an audit jointly, which is not done. Both the FIU SR and the NBS have manuals for supervision. The FIU SR may impose a pecuniary penalty or initiate the revocation of the authorisation to engage in business or other self-employed activity for the discovery of a violation. The NBS may impose a measure for the elimination and rectification of deficiencies, a financial penalty or limit or suspend the activity for the detected violations.

Of all the categories of OFIs, only in the category of payment institution, creditor and independent financial agent and financial advisor does the legislation allow for a financial penalty to be imposed on members of the management (the statutory body of the payment institution, the statutory body of the creditor and of the independent financial agent and financial adviser, a member of the supervisory board of the payment institution, the supervisory board of the creditor, a member of the statutory body or a member of the supervisory body of

the independent financial agent and financial adviser, a proxy of the payment institution, a proxy, the head of internal inspection) for breach of their obligations under Act No. 297/2008 Coll. The aforementioned procedure is regulated by the provision of § 23 (3) of Act No. 129/2010 Coll., and § 78 (11) of Act No. 492/2009 Coll., § 39 (7) of Act No. 186/2009 Coll. In other categories, only legal persons can be sanctioned for violation of AML/CFT legislation. In the case of an independent financial agent and financial advisor, also to a natural entity entrepreneur.

4.10. Licences in the OFI sector

All OFI liable persons are required to obtain a license, permit (registration), or trade license to operate. The most prudent authorisation procedure is introduced in the categories where the NBS decides on the authorisation, namely: financial agent, financial adviser, exchange bureau, payment institution, payment service provider in a limited range, payment account information service provider, payment service agent, electronic money institution and creditor. So far, there has been no refusal to issue an activity permit due to non-compliance with the AML/CFT conditions, which may also be due to the fact that statistics of this kind are not kept. If deficiencies are found in the application, the entity is invited to remedy them. In the authorisation procedure, only the category of creditors has stipulated that, together with the application for authorisation, the applicant shall also submit a programme of own activities pursuant to Section 20 of Act No. 297/2008 Coll.

In the authorisation procedure, only the category of creditors has stipulated that, together with the application for authorisation, the applicant shall also submit a programme of its own activities pursuant to Section 20 of Act No. 297/2008 Coll. Independent financial agents and financial advisors must demonstrate technical and organisational readiness in the authorisation procedure, which includes a review of the draft internal rules on measures to prevent ML of the proceeds of crime. The simplest authorisation procedure is in the leasing and factoring category, where it is sufficient for the applicant to meet the following conditions: reaching the age of 18, legal capacity and integrity, as evidenced by a criminal record extract.

4.11. Integrity in the OFI sector

In each category, when applying for a licence, permit (registration) or trade licence, it is necessary to prove integrity by submitting the information required for a criminal record extract. This condition must be met for the duration of the activity and any change must be communicated to the institution issuing the licence(s) or permit(s). Not all liable persons require new recruits to submit a criminal record certificate.

4.12. Training in the OFI sector

The majority of liable persons stated in the survey that they carry out training of employees in the area of knowledge of laws, principles and procedures in AML/CFT upon commencement of employment and subsequently at least once a year, as required by the provision of Act No. 297/2008 Coll. The majority of the inspected entities had documented compliance with this obligation during the inspections. Nevertheless, the majority of liable persons in the survey assessed the level of knowledge of their employees on AML/CFT laws,

policies and procedures as average. Testing of knowledge in this area is generally not carried out but there are exceptions, e.g. in the category of financial agent and financial adviser testing is carried out. On the other hand, there are also liable persons that provide ML/FT protection training for their employees abroad. However, there have been repeated cases in the sector where liable persons do not even know that they are liable persons and hence training is not taking place.

4.13. Security systems with AML/CFT requirements in the OFI sector

The OFI sector is predominantly made up of small entities with one or two employees, but there are also entities that consist of several branches. The organizational provision of AML-compliance system within the organizational structure of the institution, the system for determining the AML/CFT risk category of clients, the AML/CFT monitoring system of the company for the detection of UT depend on the above, but mainly on the entity of activity and the products offered. Larger entities in the survey reported that the AML compliance manager position in the institution's organizational structure has assured independence in decision-making.

For most of the entities in the OFI category, this activity is carried out by a statutory representative, as they are companies with a small number of employees. The number of employees of the institution's specialised unit for the organisational, methodological and operational provision of protection against ML/FT averages between 1 and 2 in the larger entities. All of the companies assessed in the survey reported that they had not experienced any breaches of legislation to ensure protection from ML/FT by their employees. A negligible percentage of entities use an automated AML/CFT monitoring system to check new and existing clients for being on the sanction list or the PEPs list. Many companies indicated in the questionnaire that they are able to provide this functionality with a manual system or that they are working on implementing an automated system. OFI entities predominantly use manual AML/CFT monitoring systems to detect UTs according to established criteria. The automated AML/CFT monitoring system for UT detection is mainly used by payment institutions for which it is necessary due to the nature of the services provided. According to the survey, a low number of liable persons are conducting audits to assess the effectiveness of their organisational compliance arrangements in relation to AML/CFT measures.

If the liable person identifies a low risk of ML/FT, he/she is not obliged to carry out basic, simplified or enhanced due diligence in relation to the client as it is, for example, referred to in Section 11a(1)(c) of Act No. 297/2008 Coll, which defines exemptions from client due diligence for payment services provided via a public electronic communication network without the use of electronic money, unless the value of a single transaction exceeds EUR 30 and at the same time the total monthly limit of payments made from a single telephone number does not exceed EUR 150. For example, the product of mobile operators (parking cards, public transport tickets) with registration for the provision of payment services to a limited extent, if they meet the above requirements. However, this exemption does not exempt the liable person from carrying out the monitoring of trades/business relationships so that the UT can be detected.

The highest number of UTs received was in the category of payment institutions and payment services agent, i.e. entities that provide products based on cash payments or international wire transfers, and leasing, see Table 10.

Table 10

Liable person/year	2016	2017	2018	2019
Stock exchange	0	0	0	0
FA and Financial Advisor	7	2	0	0
Exchange bureaus	5	1	0	13
Factoring	0	0	0	1
Auctions	0	0	0	0
Leasing	19	8	9	20
PI, provider of payment services in a limited range, payment service agent, electronic money institution	38	31	24	27
Creditor	0	0	0	0
Total number of UTs reported for the OFI sector	69	42	33	61

4.14. Factors influencing the susceptibility of the OFI category to AML/FT

- ✓ the total size/volume of the OFI category,
- ✓ OFI category profile based on clients,
- ✓ use of agents in the OFI category,
- ✓ the level of cash activity in the OFI category,
- ✓ the frequency of international transactions in the OFI category,
- ✓ other indicators (anonymous use of products, detection of transaction records, existence of a typology of AML, use of the OFI category in fraud or tax evasion schemes, use of products without physical presence).

The size of the sector was assessed according to the number of liable persons in each category, see Table 11 (number of authorizations in each year). The country regulates activity permits and keeps track of the number of them. However, there is no data available on the exact number of entities that also carry out the activity. However, this does not apply to FA and Financial Advisor. This phenomenon can be observed mainly in the categories of factoring, leasing, auctions and exchange bureaus. The high number of entities and the opacity of which ones are actually operating may contribute to the country's inability to provide oversight to the extent necessary to ensure that all providers are, or will be, compliant with the requirements to combat AML/FT.

Table 11

Liable person/year	2016	2017	2018	2019
Commodity exchange	1	1	1	1
FA/Financial Advisor	33,376/10	30,677/11	27,803/12	24,319/12

Exchange bureaus	1632	1641	1653	1668
Factoring	40,836	41,170	41,159	42,601
Auctions	719	713	698	701
Leasing	33,458	33,702	33,732	34,711
PI/provider of payment services in a limited range/payment service agent/electronic money institution	2/4/19/1	2/4/17/1	9/4/14/1	10/4/16/1
Creditor	32	34	31	32

Auctions and payment institutions *can be considered as the riskiest category on the basis of clients,* mainly due to the fact that the products provided by these liable persons are based on cash payments or provide the possibility to make cash payments.

According to the product analysis, the highest *ratio of international operations* is represented by products provided by payment institutions.

The ratio of other OFIs in international transactions is negligible. *Anonymous use of products* in this sector is not available. *Detecting transaction records* is easy to track in each category. *The ML/FT typology* exists more significantly in the categories: auctions, payment institutions - i.e. those where cash payment can be used. Products related to other categories are mainly used in fraud or tax evasion schemes. *The provision of products without personal participation* occurs in the category: payment institutions, electronic money institutions, creditors for products where the card payment option is used. Without personal participation, trades are also executed on the stock exchange.

4.15. Identified ML/FT threats

The biggest threat to ML/FT in the OFI sector is the provision of products or services based on making payments in cash or providing the option to make payments in cash. This option occurs, except for the stock exchange, in all categories of the sector. The restriction on cash payments pursuant to Act No. 394/2012 on the restriction of cash payments, as amended (hereinafter referred to as the "Act No. 394/2012 Coll.") does not apply to cash payments in the OFI sector in the following categories:

- exchange bureaus
- payment institutions, payment services agent and electronic money institutions,
- auctions.

Other categories of the OFI sector according to Act No. 394/2012 Coll. may accept cash payments if they do not exceed EUR 5,000,-. According to the survey carried out, liable persons try to eliminate this method of payment to a minimum or do not allow it at all on the basis of

internal regulations. On the other hand, however, the legislation allows the client to make a cash deposit into the liable person's account held with a financial institution. Here a situation arises when the employee of the financial institution in connection with a cash deposit does not sufficiently verify the origin of the deposited funds, as he/she sees that it is a payment for a product or service on the account of another liable person. Only subsequently, when the funds have already been deposited in the account of e.g. the leasing company, this reports an UT showing that the lease has been repaid early by depositing cash in the account, whereas the declared financial situation of the client at the conclusion of the leasing contract does not correspond to the fact that the lease has been repaid early. Early repayment of a lease by cash deposit into an account is the most common reason for reporting an UT by leasing or lending companies.

In the auction category, the survey found that the auction security in most cases is deposited in cash, and auctioneers do not investigate the origin of these funds. According to Act No. 527/2002 Coll., the auction security may not exceed 30% of the lowest bid but may not exceed the amount of EUR 49,790.88. The auction security shall be credited to the auctioneer as part of the price achieved by the auction. During the reporting period, the FIU SR did not receive any reports of UTs from the above-mentioned category of liable persons. In the context of depositing auction security in cash, the auctioneers themselves also see the threat of ML/FT as identified by the survey conducted.

The highest number of UTs received each year is in the category of payment institutions and payment service agent, i.e. entities that provide payment services based on cash payments or international wire transfers. According to FIU SR statistics, the greatest threat of fraud and ML/FT is in the PI and payment service agent's category.

In general, the categories of the OFI sector identified threats, i.e. the types of crime that could potentially be committed, as follows:

- financial agent/advisor – fraud, credit fraud, insurance fraud, forgery;
- factoring – tax crimes, fraud;
- leasing - tax crimes, fraud;
- PI, payment service agent, electronic money institution – fraud, phishing;
- creditor – fraud, forgery, falsification of official documents.

4.16. Identified deficiencies in the OFI category

- average knowledge of laws, principles and procedures in the fight against ML/FT by employees, but also by the liable person himself/herself,
- many entities have no knowledge of the fact that they are liable persons, despite the fact that they are obliged to comply with Act No. 297/2008 Coll., as they are not warned of this fact when they are issued a licence or authorisation to carry out their activities, and there is no reference to Act No. 297/2008 Coll. in the law that regulates their activities (this applies mainly to the following categories: factoring, leasing, auctions),
- in the sectors of factoring, leasing, auctions, exchange bureaus, there is a lack of overview on the number of entities actually operating, which may result in the country being unable

to provide supervision to the extent necessary to ensure that all providers are, or will be, compliant with AML/CFT requirements,

- there is a lack of methodological guidelines on the fulfilment of obligations arising from legislation aimed at the prevention ML/FT for individual categories, as issued by the NBS for the category of PI, payment service agent, electronic money institution,
- joint inspections by NBS supervisors and FIU SR employees are not carried out, (NBS employees would accept joint inspections in order to gain practical skills in AML/CFT inspections),
- low number of FIU SR employees, low number of NBS employees and the resulting low number of inspections carried out in relation to the number of liable persons in the OFI category,
- remote inspections are not carried out, despite the fact that Act No. 297/2008 Coll. allows it. The FIU SR does not carry out remote supervision.

5th part: Overview of priorities

General input variables according to the impact on the control mechanisms to combat AML/FT for the OFI sector were considered for each entity according to the variables:

- effectiveness of supervision/surveillance
- the availability and enforcement of administrative sanctions
- the availability and effectiveness of input control mechanisms
- knowledge of the fight against ML by business/institution employees
- effectiveness of the compliance function (organisation)
- the effectiveness of monitoring and reporting suspicious activities
- the comprehensiveness of the legal framework in the fight against ML/FT
- the availability of a reliable identification infrastructure
- the availability of independent information sources
- honesty of the employees of the business/institution

6th part: Proposals for measures

The following measures should be taken to improve the variables that need to be given increased priority:

a) employee knowledge of AML laws, policies and procedures

- intensify the methodological and training activities of the FIU SR and the NBS
- development of a knowledge test on Act No. 297/2008 Coll. and procedures in the fight against ML/FT, which would be available on the FIU SR website
- tighten the liable person's procedures for verifying the knowledge of his/her employees
- focus more on the content and quality of the training process and the subsequent verification of employees' knowledge in the FIU SR's control activities

b) the effectiveness of AML/CFT surveillance

- increase the staffing levels of both the FIU SR and the NBS - to be followed by an intensification of inspections
- make use of the possibility to carry out inspections or supervision remotely, as the law allows it but it is not used; the NBS carries out supervision remotely
- improve cooperation between FIU SR and NBS inspection authorities, carry out joint inspections, the law allows, but they are not carried out

c) the effectiveness of compliance functions

- draw up methodological guidelines on the fulfilment of the obligations of persons responsible for AML/CFT arising from legislation aimed at the prevention of ML/CT for each category, indicating the methods and forms of AML/CFT for each category

d) the effectiveness of UT monitoring and reporting

- draw up methodological guidelines on the fulfilment of the obligations of persons responsible for AML/CFT arising from legislation aimed at the prevention of ML/FT for each category, indicating the methods and forms of AML/CFT for each category

e) the availability and applicability of administrative and criminal sanctions

- increase the number and amount of fines imposed, to apply in practice criminal sanctions for serious breaches of AML/CFT legal standards
- increase the general awareness of liable persons and their employees of the criminal consequences of violating AML/CFT legal standards
- also sanction individuals for breaches of AML procedures

11. INSURANCE SECTOR

At the end of 2019, there were 13 insurance companies with its registered office in the Slovak Republic established in the Slovak insurance market, 20 insurance companies from another EU Member State that carried out insurance activities in the territory of the Slovak Republic through a branch (including 5 in the life insurance sector) and 541 insurance companies from another EU Member State that carried out insurance activities in the territory of the Slovak Republic on the basis of the free provision of services without establishing a branch.

In terms of asset size of financial market entities, insurance companies accounted for 7.1% of the financial market as of 31 December 2019.

The size of the value of the product in the insurance sector is mainly determined through written premiums.

As of 31 December 2019, the total volume of premiums written in accordance with Solvency II legislation was EUR 2,523,108 thousand, while the volume of premiums written in life insurance was EUR 1,180,058 thousand (46.8%) and in non-life insurance EUR 1,343,349 thousand (53.2.8%). Investment life insurance, amounting to EUR 343,813 thousand, represented 29.1% of the life insurance business as of 31 December 2019.

Conclusions from the previous NRA

The analysis of the information obtained in the framework of the supervision/inspections as well as from the questionnaires submitted by the liable persons in the framework of the NRA1 for the period 2011-2015 revealed a number of shortcomings.

One of the shortcomings pointed out by the NRA1 report was the absence of a sub-legislative regulation in the legal system (e.g. a decree or a measure), which would specify in more detail the different areas and the content of the obligations for insurance companies, which are generally regulated in the AML Law. The NBS Methodological Guideline is only of a recommendatory and non-binding nature. This shortcoming was eliminated by the amendment of the AML Act by adding a new paragraph 5 to Section 20 of Act No. 279/2020 Coll. with effect from 1 November 2020, which allows the NBS, after consultation with the Ministry of the Interior of the Slovak Republic, to issue a generally binding legal regulation, whereby it establishes for liable persons, which are subject to the supervision of the NBS, the requirements for the elaboration, implementation, updating and application of the programme of own activities and the assessment of risks pursuant to Section 20a, and other details related to the programme of own activities and the assessment of the risks.

The processing of the information submitted during NRA 1 revealed that the NBS and the FIU SR carried out supervision/inspection focusing on AML for a very small number of insurers as liable persons. Also, the FIU SR imposed only a small number of sanctions on insurance companies for breaches of the AML Act in the period under review and the NBS did not impose any sanctions. Since 2018, the NBS has carried out an increased number of on-site supervisions aimed at inspecting insurance companies in fulfilling and complying with the

obligations laid down by the AML Act, with 5 thematic supervisions focused on the supervision of AML, in which no sanctions were imposed.

In order to prove the integrity of employees, the NBS recommended insurance companies to require from their employees not only an extract from the criminal record, but also a declaration of honour of certain facts proving their integrity, or other necessary documents, including the submission of an employment report from a previous employer. Some insurance companies differentiate in proving the integrity between individual positions (e.g. persons responsible for a key function, employees of the liquidation department, financial operations department, etc.) where they have defined the conditions for proving integrity more broadly and, on the other hand, positions for which they only require employees to have a criminal record statement.

Some insurance companies do not have specific statistics on the number of internal inspections aimed at detecting deficiencies (failures of employees) resulting from non-compliance with their AML obligations, even in the 2016-2019 assessment period.

Another finding within NRA1 was a finding relating to the AML officer who was not classified as a senior member of staff. Following the amendment of the AML Act by Act No. 52/2018 Coll., which directly stipulated in Section 20(2)(h) that if such person is not a statutory body or a member of a statutory body, the person responsible for the AML area must be a senior employee, insurance companies have placed the said person in the position of a senior employee.

The NBS also recommended insurance companies to include internal and external audits in the control plan. Although internal audits are carried out regularly once a year in most insurance companies, external AML audits are carried out on an exceptional basis.

Further, it was found during NRA1 that the requests of the insurance companies for data and documents within the meaning of Section 13(1) of the AML Act regarding the verification of the information found by the insurance companies in the course of the exercise of diligence in relation to the client were not accepted by the banks. This mainly involved verifying the details of the owners of the relevant contact bank accounts mentioned in the insurance contracts. During the 2016-2019 evaluation period, it was found that this situation persisted.

The analysis of the exit forms as well as the on-site supervisions carried out during the assessment period 2016-2019 revealed that **some insurance companies and branches of insurance companies from another EU Member State, as liable persons, continue to:**

- identify the BO but do not take reasonable steps to verify the identification of the end-user,
- not classify clients into risk groups, lack a risk-based approach,
- not carry out any inspection aimed at the fulfilment of AML obligations, or with a significant time lag, the AML system and processes are not subject to an internal audit at least once a year in accordance with the NBS Methodological Guideline No. 5/2019,
- do not carry out ongoing monitoring of the business relationship.

Deficiencies resulting from UT reporting (including persistent):

- due diligence is not consistently carried out in relation to the client, in some cases complete basic due diligence is completely absent,
- when assessing trades, there is no emphasis on identifying the origin of funds at the entry to the system, UT reporting is focused only on the exit of funds (underwriting, termination of insurance) from the insurance segment,
- in the case of tracing the origin of funds, only the declaration of honour of the client shall be applied,
- UT reports do not include information from basic due diligence already carried out,
- inadequate description of the unusuality in the reported trade as well as overall misidentification of the unusuality (e.g. incorrect reason for the unusuality, international arrest warrant of the client or non-payment of the payment specified in the contract),
- inadequate assessment of individual trades (exceptionally high deposits).

In most cases, insurance companies still do not use automated systems to monitor UTs, nor do they use automated monitoring to check sanction lists and PEPs.

Analysis of risks, process vulnerabilities

AML/CFT legislation in the insurance sector

The AML Act transposing Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of ML/FT is the basic legislation regulating the AML area for all liable persons, including supervised entities in the insurance sector. In order to implement the recommendations of the Moneyval Committee of the Council of Europe contained in the Fifth Evaluation Report on the implementation of measures against money laundering and financing of terrorism in the Slovak Republic, as well as the revised recommendations of the FATF (Financial Action Task Force of the G7), it will be necessary to amend the AML Act.

At the same time, the insurance sector is also regulated by Act No. 39/2015 Coll. on Insurance and on Amendments and Additions to Certain Acts, as amended (hereinafter referred to as the "Insurance Act") as a specific legislation.

The AML issue is indirectly related to Act No. 171/1993 Coll. on the Police Force, Act No. 101/2010 Coll. on Documenting the origin of the property, Act No. 91/2016 Coll. on the criminal liability of legal persons, the Criminal Act, the Criminal Procedure Code and international treaties to which the Slovak Republic is bound.

A more detailed explanation on the fulfilment of obligations arising for supervised entities in the insurance sector from the AML Act and the Insurance Act is contained in the Methodological Guidance of the National Bank of Slovakia Financial Market Supervision Units of 9 May 2019 No. 5/2019 on the protection of an insurance company, a branch of an insurance company from another EU Member State and a branch of an insurance undertaking from a non-EU Member State in the conduct of life insurance business against the ML/FT (hereinafter referred to as the "Methodological Guideline"), which replaces the previous Methodological Guideline of 4 October 2013 No. 4/2013. The Methodological Guideline includes two annexes containing Guidelines on Risk Factors Associated with Client Relationships and Occasional Transactions (Annex 1) and General and Specific Ways to Recognise Unusual Business

Transactions(Annex2).
http://www.nbs.sk/_img/Documents/_Legislativa/_Vestnik/MU_5_2019.pdf.

The methodological guidelines issued by the FIU SR are published on www.minv.sk/?informacie-a-usmernenia-pre-povinne-osoby-a-zdruzenia-majetku.

It follows from the above that the AML legislation for the insurance sector is comprehensive, but there is no sub-legislation (e.g. decree or measure) that would specify in more detail the individual areas and the content of the obligations for insurance companies, which are generally set out in the AML Act. The methodological guidelines of the NBS and the FIU SR are only of a recommendatory, non-binding nature and are not legally enforceable.

Effectiveness of supervisory practices and methods (NBS and FIU SR)

Supervision/surveillance of institutions in the insurance sector is carried out by the FIU SR as well as by the NBS. The primary objective of supervision/inspection is to promote the elimination or mitigation of each type of potential ML/FT risk in supervised entities.

The NBS performs:

- **comprehensive supervision** - oversight of the company's overall operations, detailed, analytical,
- **thematic supervision** - supervision of selected company activities (e.g. investment services, AML, compulsory contractual insurance),
- **tracking supervision** – checking the measures taken to address deficiencies identified during comprehensive or thematic supervision, i.e. inspection of the implementation of the action plan adopted by the insurance undertaking to remedy the deficiencies.

AML screening is carried out by the NBS as part of comprehensive supervision (or tracking) or separately as thematic supervision.

TYPE of supervision	2016	2017	2018	2019
comprehensive	0	1	0	0
thematic supervision on AML	0	0	2	3
tracking supervision on AML	0	0	0	0

Number of supervisions of insurance companies by the NBS

Since 2018, the NBS has carried out an increased number of on-site supervisions aimed at inspecting insurance companies in fulfilling and complying with the obligations laid down by the AML Act, with 5 thematic supervisions focused on the supervision of AML being carried out. At the same time, by adopting an internal regulation focused on risk-oriented supervision in March 2018, the NBS increased the frequency of remote supervision of all insurance companies in the area of AML in the form of questionnaires, which are sent to insurance companies and subsequently evaluated every 2 years.

During the on-site supervisions carried out by the NBS during the assessment period, the following deficiencies were detected in the inspected insurance companies:

a) minor deficiencies
- shortcomings and findings in the own activities programme
- the absence of documents demonstrating the assessment of the risk of ML/FT, on the basis of which the insurance company determined the scope of due diligence for the clients of the insurance contracts in question
- the insurance company's system and processes for the prevention of ML/FT were not subject to internal audit in 2016, 2017 or 2018

b) serious deficiencies
- in some of the UT reports for FIU SR, persons were listed as the designated person, none of whom had been designated as the designated person under section 20(2)(h) of the AML Act by the insurer's statutory body during the period in question
- for some insurance contracts it was not proven whether the insurance company had verified the identification of the client, who is a legal entity, and none of the insurance contracts fell into the category of the exercise of simplified due diligence under Section 11 of the AML Act
- certain business transactions, due to their unusual nature, should have been subject to the insurance company's assessment under Section 14(1) in conjunction with Section 14(2)(a) of the AML Act, whereas there was no document in the files of the contracts in question demonstrating the assessment of the business transactions in question from the point of view of their unusual nature and the insurance company was therefore unable to demonstrate that it had complied with this obligation

c) very serious deficiencies
- for some insurance contracts where simplified diligence cannot be applied due to the high value of the business, the identification of the BO and the adoption of appropriate measures to verify his/her identification have not been carried out
- a number of insurance policies identified trades that were unusually large and clearly outside the normal scope of trades conducted by policyholders, as well as trades that also had no apparent economic purpose and thus should have been reported to the FIU SR as UT, and the insurance company failed to document review and assessment of certain trades. At the same time, the insurance company did not fully carry out ongoing monitoring of business relationships pursuant to Section 10(1)(g) of the AML Act.

At the end of 2019, one insurance company was sanctioned by the NBS on the basis of deficiencies detected during on-site supervision.

The FIU SR did not carry out any inspections of insurance companies as liable persons and did not impose any sanctions during the period under review.

At the same time, it should be noted that this situation is linked to the insufficient staffing of the FIU SR Inspection of Liable Persons Department (mainly professionally competent staff), which made it impossible to carry out a sufficient number of inspections of the liable persons in this sector during the period under review.

In addition to performing on-site inspections of liable persons and conducting administrative proceedings for violation of the AML Act, the Inspection of Liable Persons

Department also participates to a considerable extent in legislative processes related to the AML Act, methodological, training and administrative-legal activities related to the performance of the tasks of the FIU SR, as well as in the Fifth Round of the evaluation of the Slovak Republic by the Moneyval Committee.

Initial inspections - permitting procedures prior consents, notification obligations

The comprehensive legal and regulatory framework provides the NBS with appropriate powers to carry out initial inspections as part of the authorisation procedure, the procedure for granting prior approval for the acquisition or increase of a qualifying holding in an insurance company, the procedure for granting prior approval for the merger, amalgamation, division of insurance companies, as well as the procedure for granting prior approval for the sale of the undertaking of an insurance company or a part of it. Insurance companies are also obliged to notify the NBS without undue delay of any changes in the persons managing the insurance company, branch of the insurance company or performing key functions (Solvency II regime) and persons proposed as members of the board of directors and senior employees under the direct management responsibility of the board of directors (special regime), including all information and documents necessary to assess whether the new natural entity meets the requirements of professional competence and credibility.

As part of the authorisation procedure, the NBS examines the demonstration of:

a) the transparent and credible origin of the capital and other financial resources of the insurance company,
b) the suitability of persons with qualifying holdings in the insurance company,
c) the transparency of a group with close links, which includes a qualifying shareholder in an insurance company,
d) whether the exercise of supervision is hindered by close links within the group,
e) the competence and trustworthiness of the persons who are proposed to manage the insurance company or who will have key functions that are part of the corporate governance system, which are at least the risk management function, the compliance function, the internal audit function and the actuarial function (Solvency II regime), the competence and trustworthiness of the persons proposed to be members of the board of directors and senior staff under the direct management responsibility of the board of directors (special regime),
f) whether the exercise of supervision is impeded by the law and the manner in which it is applied in the State in the territory of which the group with close links has close links ,
g) the ability to comply with the system of corporate governance in accordance with the relevant provisions of the Insurance Act,
h) the capital requirements laid down by the Insurance Act.

The suitability of persons with qualified participation in the insurance company, as well as the fulfilment of the conditions referred to in points (c), (d) and (f), shall be examined by the NBS not only in the framework of the authorisation procedure, but also in the framework of the procedure for granting prior approval pursuant to Section 77(1) of the Insurance Act.

The method of proving compliance with the conditions for granting a permit to carry out insurance activities, as well as the conditions for granting prior approval pursuant to Section 77(1) of the Insurance Act, is regulated by implementing legislation issued by the NBS (NBS Measure No. 5/2015, NBS Measure No. 8/2015 and NBS Measure No. 35/2015). With regard to the existence of adequate resources to ensure the quality of the implementation of initial inspections, NBS considers that all documents and data are competently examined and evaluated by the employees of the Authorisation Department and that authorisations as well as previous approvals are granted on the basis of a sufficient demonstration of compliance with the conditions laid down by the Insurance Act. In the same way, the competent employees shall competently assess and evaluate the demonstration of compliance with the conditions laid down by the Insurance Act outside the proceedings, if the subject of the review are reporting obligations.

In the period under review, the NBS granted 8 previous approvals in the insurance sector, while in the period 2016-2019 the NBS did not receive any applications for authorisation to carry out insurance activities.

Employee credibility in the insurance sector

The condition of credibility of employees of insurance companies is normally regulated by the internal regulations of insurance companies, e.g. Conditions of employment, Code of Ethics, Anti-Corruption Regulations, etc., with the proviso that most insurance companies require not only an extract from the criminal record, but also a declaration of honour of certain facts proving credibility, or other necessary documents, including the submission of an employment reference from a previous employer, in order to prove the credibility of the employees.

In the case of persons managing the insurance company or performing key functions (Solvency II regime) and persons nominated as members of the board of directors, proxies and senior employees under the direct management responsibility of the board of directors (special regime), the insurance company verifies the fulfilment of the requirements for professional competence and credibility in accordance with the provisions of Section 24 or Section 181 of the Insurance Act. Insurance companies are obliged to notify the NBS without undue delay of changes in these persons, including all information and documents necessary to assess whether the new natural entity meets the requirements of professional competence and credibility.

The rules of conduct of their employees to prevent conflicts of interest, insider trading or misuse of confidential information are by default regulated by insurance companies in internal regulations, which are updated from time to time, with accessibility for all employees generally provided by means of an intranet.

In accordance with Section 20(2)(i) of the AML Act, insurance companies have a mechanism within their internal regulations, i.e. in the programme of own activities, for the protection of employees from the negative consequences and risks resulting from the reporting of UTs.

Statistics on the number of internal inspections aimed at detecting deficiencies (failures of employees) resulting from non-compliance with their AML obligations are still not in place for some insurance companies.

With the exception of two insurance companies, no suspected intentional crimes of a property nature committed by employees were reported by insurance companies during the period under review. With the exception of two insurance companies, insurers did not report any employees who violated internal rules to prevent conflicts of interest, insider trading, or insider abuse. None of the insurance companies filed a criminal complaint against the employee in connection with the AML violation.

AML/FT employee knowledge in the insurance sector

The own AML programme regulates the training of employees in insurance companies, including a system of training and coaching activities. The system of training and coaching activities varies, depending on the particular insurance company, with the proviso that the training is compulsory and aims to ensure that employees acquire the necessary knowledge of the insurance company's AML/CFT programme and the AML Act.

The following training is carried out within individual insurance companies**:**

a) new recruits - initial training,
b) once a year e-learning training - all employees; some insurance companies have once a year training only for employees in selected positions,
c) enhanced training for specific departments whose employees may be more exposed to opportunities and attempts of abuse for ML/FT purposes,
d) training of financial intermediaries.

Each employee undergoing training is required to pass a knowledge test to test their knowledge of AML, with insurance companies having a set percentage of passing the test (standard 70% - 85%). Training of new as well as permanent employees is mainly carried out in the form of e-learning. Insurance companies have AML training materials and regulations stored on their intranet and available to all employees at all times. With the exception of a few insurance companies, AML training materials include a warning about the criminal consequences of violating AML legal standards. In addition to internal trainings, insurance companies allow their employees to regularly participate in external trainings organised by e.g. NBS, FIU SR, etc.

The overall level of employees' knowledge of AML obligations (in particular the obligation to report UT, the ability to assess situations where there is an increased risk of AML, understanding of the legal consequences in the event of a breach of obligations under the AML Act) was most often rated by insurance companies with a score of 2 (on a numerical scale of 1 - 5, best - 1, worst - 5). The numerical rating of 2, on the one hand, reflects the knowledge of employees of the obligations under the AML Act, while, on the other hand, it takes into account certain shortcomings, in particular in the areas of client categorisation, the detection of BOs, the monitoring of PEPs and sanctioned persons.

Organisation of compliance in the insurance sector

Insurance companies have a clear and transparent division of AML competences and responsibilities within their organisational structure. The overall protection of insurance companies against ML/TF is the responsibility of the Board of Directors of the insurance companies, with a designated person who is under the direct management responsibility of the CEO or the Board of Directors and is fully replaceable by his/her representative(s) being responsible for the practical implementation of the activities in the above-mentioned area. The separation from operational and commercial activities ensures the independence of its function. Necessary independence means that the compliance function cannot be subject to any undue pressure in relation to reporting, targets, target setting, remuneration or otherwise. The compliance function (or relevant employees) also has an unrestricted right to communicate with all employees and has access to all information, records or data necessary to carry out its duties within the limits defined by law. Management as well as all persons concerned are liable to provide the compliance function with all relevant information.

The organisational arrangements for the AML agenda in insurance companies are as follows:

a) a separate organisational unit - the Compliance Department,
b) the Compliance Department as part of the Legal and Compliance Department,
c) only the responsible employee designated in the organisational structure (small insurance companies) or 2 employees.

In most insurance companies, the position of the person responsible for AML is part of the key compliance function under the Insurance Act and therefore must meet the professional competence and credibility requirements in accordance with Section 24 of the Insurance Act. Similarly, if the person responsible for AML is in a senior management position under the direct management responsibility of the board of directors, he/she must meet the above requirements. The number of employees of insurance companies that provide AML agenda ranges from 1 to 4 employees, depending on the size of the insurance company. It can be concluded that the majority of insurance companies have sufficient staff resources.

The basic internal regulation for the methodological provision of AML in insurance companies is the AML Programme, which is intended for all employees. The AML regulation contains an explanation of basic definitions and terms, AML/CFT legislation, client/product/trade-specific AML/CFT risk assessment, how to conduct and types of due diligence in relation to the client, an overview of the forms of UT, a description of the procedure and principles for reporting and assessing UT, and the data retention procedure, the definition of the responsibilities of individual employees, including the designation of the person responsible for AML/CFT, how to ensure the protection of the employee who identifies UTs, the content and timing of training for employees who may come into contact with UTs in the course of their work, as well as the control mechanisms for compliance with these provisions and obligations.

AML information flows

The person responsible for AML directly reports on his/her activities to the company's Board of Directors, the CEO, the Audit Committee (if the insurance company is a member of a group, also to the group's compliance unit) at least once a year and provides information immediately in the event of serious deficiencies being identified. Employees are required to inform the person responsible for AML of possible suspected UTs. The person responsible for the AML shall then assess the possible unusualness of the transaction and, if it shows signs of unusualness, report the transaction to the FIU SR without undue delay. The protection of information is ensured on the basis of the obligation of confidentiality imposed on employees by internal legislation and continues after termination of employment.

The number of audits in insurance companies focused on AML varies depending on the specific insurance company, usually once a year, while in the period under review only internal audits were carried out in insurance companies, with the exception of one insurance company where the external audit also partially covered the AML area.

Availability and enforceability of administrative sanctions in the insurance sector

The regulation of administrative sanctions is contained in Section 32 - Section 34 of the AML Act, as well as in Section 139 - 159 of the Insurance Act.

The range of sanctions that the NBS is authorised to impose on insurance companies under the Insurance Act is wide and includes, for example, corrective measures, fines ranging from EUR 1,000 to EUR 1,000,000, restriction or suspension of activities, restriction or prohibition of free disposal of assets, with the most severe sanction being the withdrawal of the authorisation to carry out insurance activities. In the case of minor deficiencies, the NBS shall be entitled to discuss the deficiencies in the activity of the insurance or reinsurance companies with members of the board of directors of the insurance company or with the head of the branch, with members of the supervisory board of the insurance company, with senior employees or persons who have key functions, who are obliged to provide the National Bank of Slovakia with the assistance required by the NBS, also outside the proceedings on the imposition of a sanction or a measure.

In accordance with Section 139(6) of the Insurance Act, a fine may also be imposed on a member of the board of directors, a member of the supervisory board, the head of a branch, a receiver, a proxy, up to 12 times the monthly average of his/her total income from the insurance company. It is also possible to impose a fine on persons other than those listed above who manage the insurance company or on individuals who have key functions, up to 50% of twelve times the monthly average of their total income from the insurance company.

However, in application practice, no such sanctions were imposed in the period under review.

The FIU SR may impose a fine of up to EUR 1.000.000 or up to EUR 5.000.000 on the liable person for non-compliance or violation of the obligations arising from the AML Act pursuant to Section 33 of the AML Act, or up to EUR 5.000.000 in the case of a bank and a

financial institution. Pursuant to the provisions of Section 33a of the AML Act, in addition to the fine for the administrative offences referred to in Section 33(1) and (2), the financial reporting unit may also impose on a legal entity or entrepreneur the sanction of disclosing the final decision on the imposition of the sanction.

Pursuant to the provisions of Section 34 of the AML Act, if the liable person fails or repeatedly fails to fulfil or violates the obligations laid down in the AML Act for more than 12 consecutive months or repeatedly, the FIU SR shall file a petition for revocation of the authorization for entrepreneurial or other self-employed activity with the authority authorized to decide under a special regulation.

In the period under review (2016-2019), no sanctions were imposed by the NBS and the FIU SR on insurance companies relating to AML issues.

Unusual transactions

a) Forms of UT

The definition of UT under Slovak law is based on a demonstrative enumeration of the general forms of UT (Section 4(2) of the AML Act).

Considering the wide range of liable persons, the legislator could not define by the AML Act all possible UTs that occur in the performance of individual activities covered by the Act, therefore, it obliged liable persons to develop and update the programme of own activities and to determine their own forms of UTs according to the subject of their business activities. This also applies to the insurance sector. The forms of UT by activity and type of business carried out are part of the insurance company's own business programme pursuant to Article 20(2)(a) of the AML Act.

Insurance companies, as liable persons, are also obliged to assess, in accordance with the provisions of Section 14(1) of the AML Act, whether the transaction being prepared or carried out is unusual. Therefore, insurance companies must have regulated the assessment of the unusualness of transaction in their own business programme so that it is absolutely clear which persons assess the unusualness of the transaction being prepared or executed within their own structure, the time at which these persons carry out the assessment in question and the manner in which the assessment is carried out (in particular, by comparison with a review of the forms of UTs, etc.). Assessments should also be made on the basis of other information identified by employees from available information e.g. risk profile, open sources with regard to the risk of ML/FT.

The assessment of UT is carried out by insurance companies from two perspectives:

a) the riskiness of the client - under the "know your customer" principle - KYC (entity types, territorial risk)
b) the nature, type, duration, content and manner of carrying out the transaction.

In particular, the following cases are considered to be signs of UT in the insurance sector:

- if the client refuses to provide identifying information or data necessary to carry out the due diligence, or refuses to declare on whose behalf he/she is acting,
- entering into a transaction with a client who, because of his/her occupation, status or other characteristic, may be presumed not to be, or not to be in a position to be, the owner of the necessary funds,
- if the amount of funds at the client's disposal is manifestly disproportionate to the nature or extent of the client's business or the client's declared assets,
- entering into a transaction where there is a reasonable expectation that the client or BO is a person subject to international sanctions or a person who may be related to a person subject to international sanctions, or the item or service is an item or service subject to international sanctions,
- a transaction in which the client presents false, invalid or stolen identification documents,
- the client's interest in taking out an insurance policy in an amount that appears to be inconsistent with the client's insurance needs,
- the client accepts terms and conditions that are unfavourable to him/her and have no relation to his/her health or age, and is willing to pay premiums that are clearly beyond his/her financial means,
- the client buys an insurance product that has no obvious economic purpose and is unwilling to give a reason for the investment when asked by an insurance company employee,
- repeated conclusion (3 or more) of insurance contracts for unusually high amounts,
- the client changes the beneficiaries designated in the contract, often to a beneficiary who has no clear link to the policyholder,
- the claimant shows no interest in the performance of the contract when the contract is entered into, but shows much more interest in the early cancellation of the contract, and it may appear that the claimant has insurance with more than one insurance companies,
- the client requests an extreme increase in the sum insured and the premium,
- the client makes multiple account changes for payment and refund of premiums,
- one client concludes multiple insurance contracts for the benefit of multiple insured persons,
- very short period (up to 3 months) between the conclusion of the contract and its cancellation for high sums insured,
- arranging insurance where the annual premium is an unusually high amount,
- the client pays a high sum insured in cash or by postal order,
- a deliberate error in entering the payment identification or the client, after the funds have been paid into the insurance company's account, subsequently notifies the insurance company that a mistake has been made and asks for the funds to be sent back to him/her, either to another account or by postal order,
- the client pays approx. two instalments and then asks for the amount to be paid into another account,
- after regular premium payments, the client makes a one-off payment of the entire premium at once, or transfers funds from several banks, especially from abroad,

- for investment products, the client makes three or more recurring deposits by wire transfer to the account.

b) Method of conducting the UT assessment

Information obtained from insurance companies showed that most insurance companies carry out UT monitoring manually. Some insurance companies perform monitoring in a semi-automated way, i.e. manually and through electronic reports generated on a monthly basis after manual entry of specified parameters into the insurance company's operating system.

The assessment of UTs by automated means is performed minimally in practice, only by so-called post-transactional monitoring, after a manual assessment has been carried out. However, several insurance companies declared that they are working on the development of automated systems. Some insurance companies with a small volume of business in the market, or those offering only non-life insurance, do not set AML risk categories.

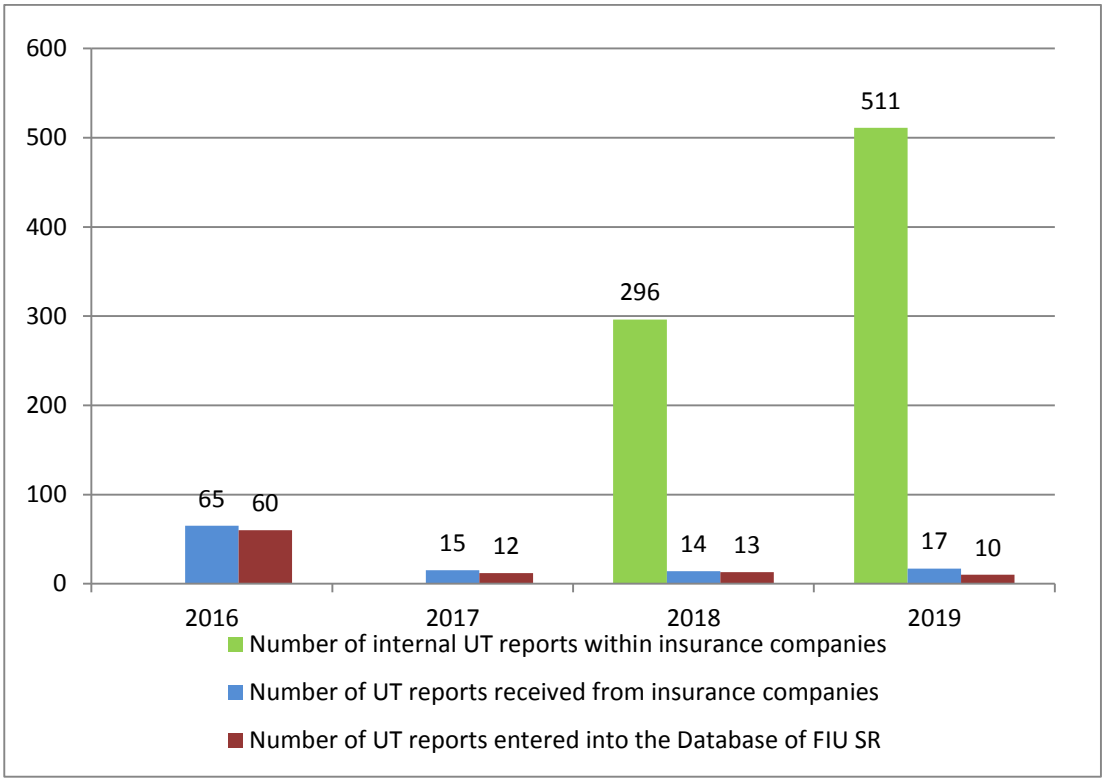
Most insurance companies will select and execute the appropriate due diligence in relation to the client in each business transaction. For each transaction, it assesses whether it exhibits the characteristics of a UT according to the 'know your client' principle and the overview of the forms of UT set out in the relevant internal rules of the individual insurance companies. As a rule, the responsible employee manually evaluates the business operation and, in case of suspicion, completes an internal "UT Report", which is sent to the Compliance Department by e-mail, fax or post without undue delay. The department concerned, after assessing the unusuality through the designated person, shall send the UT report to the FIU SR without undue delay.

c) Effectiveness of UT monitoring and reporting

Of the total number of reported UTs from all liable persons, the FIU SR records the highest number of UTs (approx. 85-90%) from banks, where the largest number of trading operations, including cash operations, are concentrated.

Insurance companies

Year	Accepted		Retrieved from				
	UT in total	of this from insurance companies	National Crime Agency (NAKA)	RH PF, DH PF	FD SR	FIU SR	DTB
2016	3,297	65	2	1	2	0	60
2017	2,636	15	1	0	1	1	12
2018	2,509	14	1	0	0	0	13
2019	2,576	17	1	4	2	0	10



Dynamics of the development of the number of UT reports in the insurance sector and the efficiency of their use

(Note: the data provided by one insurance company regarding internal reporting for 2016 and 2017 were not sufficiently correct for use in this table due to their high bias, which would seriously affect the statistics of the whole module)

However, it was not clear from the majority of the above-mentioned reports for what reason the transaction in question was assessed as unusual (incorrectly identified possibility of unusualness of the transaction), nor whether and what due diligence (or scope of due diligence, performance of "repeated" due diligence) was performed by the liable person in relation to the client (ascertaining the origin of the funds, the BO, etc.), i.e. the due diligence in relation to the client was performed by a number of insurance companies in an inconsistent manner, or the reports did not contain the information ascertained from the due diligence carried out.

The analysis of the UT reports showed that a significant part of the reported business transactions could have been assessed by the insurance companies in their own competence as usual business transactions, or some should not have been reported as UTs at all. In most cases, insurance companies reported all transactions that fulfilled one of the forms of UT listed in their own programme of business without re-performing the appropriate **due diligence** in relation to the client and assessing comprehensively the unusualness of the business transaction carried out, including the use of the KYC principle.

Again, insurance companies did not investigate the origin of funds entering the financial system, allowed this entry of "possible" illegal sources, and then reported as UT only the exit of funds from the system (surrender, cancellation of insurance).

Overall sector riskiness

In terms of ML/FT, the insurance sector can be assessed as less attractive compared to the banking sector. Funds related to insurance contracts (premiums, claims payments) are directed from/to client accounts held with other financial institutions that are liable entities under the AML Act. Only some insurance products (e.g. travel insurance, accident insurance, compulsory contractual insurance) are paid in cash (even to a limited extent), with the extent of cash acceptance in the Slovak Republic being completely negligible in relation to the total volume of premiums received. Insurance companies use not only an internal but also an external network, i.e. financial intermediaries, to sell their products. However, it should be stressed that the ultimate responsibility for exercising complete due diligence in relation to the client rests with the insurance company (strict liability), despite the fact that financial intermediaries are also classified as liable persons under the AML Act.

More than 70% of production in the insurance sector is offered through financial intermediaries.

When assessing the level of ML/FT threat in the insurance sector, it is essential to distinguish between non-life and life insurance products. The application practice shows that the use of non-life insurance products for ML is minimal and therefore the level of ML threat can be described as insignificant. The level of the threat of FT for non-life insurance products is moderately significant.

Compared to non-life insurance, the level of ML/FT threat in life insurance poses a higher risk, especially for investment life insurance. The increased ML risk in investment life insurance products arises mainly from the possibility of investment by clients in the form of single deposits or recurring deposits and withdrawals. These products are primarily linked to the investment component of the contract and not to the traditional insurance risk (death, survival). The nature of insurance products in life insurance requires relevant expertise and therefore less sophisticated products in other sectors, e.g. banking products, are more often used in practice for ML/FT purposes. Hence, the level of ML/FT threat for life insurance products can be assessed as moderately significant.

ML/FT risk is assessed by insurance companies depending on the client, the product (life or non-life insurance product), the business relationship or the specific business, taking into account the AML Act and internal AML regulations when assessing risk. However, two insurance companies stated that the risk assessment of clients as well as the risk assessment of products will be the subject of internal regulations they are currently preparing.

a) ML/FT risk assessment of clients

As part of the risk assessment of clients, insurance companies classify clients into three or four risk categories and then, according to the risk category, carry out the appropriate type of due diligence towards the clients. The exception is one insurance company which, due to the nature of the insurance products sold, classifies its clients in the low-risk category.

For life insurance products, insurance companies periodically review the risk classification during the course of the business relationship, with the risk classification changing in the event of new information about the client and his/her transactions (e.g. an unusual change in the insurance contract, the execution of an occasional trade above EUR 15,000, etc.). Updates are also made on the basis of the client completing the relevant form at least once per calendar year. For non-life insurance products, there is no reassessment of clients' AML risk categories during the course of the business relationship.

As a rule, insurance companies consider a **client to be less risky** from the point of view of ML/FT, in particular if the client is:

- a bank or financial institution under the AML Act (e.g. insurance company, securities dealer, etc.),
- a public authority of the Slovak Republic (e.g. the Ministry),
- municipality, city.

In particular, a client may be considered a **higher risk client** in terms of ML/FT if the client is:

- a person of whom the responsible person has knowledge that he/she is or has been suspected of criminal activities, in particular of a pecuniary or economic nature (e.g. theft, embezzlement, fraud, unjust enrichment, usury, tax evasion, etc.),
- long-term unemployed person with no income,
- a person employed or conducting business in an area with a higher risk of ML/FT (e.g. money exchange bureaus, betting shops, gambling shops, etc.)
- a person permanently resident outside a Member State of the European Union,
- a person who is not a citizen of a member state of the European Union,
- an alien, in particular a natural or legal entity, whose country of origin (citizenship, residence, domicile) does not sufficiently apply measures against the legalisation of proceeds,
- a person at higher risk of corruption (decision-maker, public official),
- a person with outward signs indicating membership of extremist groups and movements,
- a person who presents to the responsible person documents suspected of being forged, altered or lost,
- home-less person,
- shell company,
- a legal entity with an opaque ownership structure,
- a company that frequently changes its name and registered office,
- legal entity - a pool of assets (e.g. foundation, non-profit organisation, non-investment fund),
- PEP,
- a person on the list of sanctioned persons.

To identify and verify the identification of clients, insurance companies use publicly available sources such as commercial and trade registers, internet browsers, DOW JONES portal, GIN2ACT portal of the company in order to verify persons in terms of PEP, embargos and sanctions

http://ec.europa.eu/taxation_customs/taxation/gen_info/good_governance_matters/lists_of_countries/index_en-htm.

Insurance companies use publicly available sources (e.g. commercial register, register of public sector partners, register of accounts, FinStat, etc.) to identify and verify the BOs, regardless of their risk category, and most insurance companies also require the submission of a declaration of honour.

Politically exposed persons (PEPs)

Most insurance companies do not use a special monitoring system to determine whether new and existing clients are on the sanction list or are PEPs and inspect clients manually or in a semi-automated way via excel. In order to verify persons, insurance companies use publicly available sources and internet browsers containing lists of persons subject to international sanctions. Some insurance companies maintain lists of PEPs and sanctioned persons, which they update from time to time. Most insurance companies require declaration of honour of clients that they are not PEPs when taking out insurance policies and then check at least once a year during the term of the insurance contract that this condition is met.

b) ML/FT risk assessment of insurance products

The assessment of the insurance sector in terms of AML focused on life insurance and non-life insurance, despite the fact that according to Article 5(1) of Act No. 297/2008 Coll., an insurance company is a liable person for the purposes of this Act when carrying out insurance activities only in life insurance. Within life insurance, investment life insurance (unit-linked) was assessed separately as an insurance sector in which an increased risk of money laundering and risky life insurance (death insurance, endowment insurance, pension insurance) was identified. The increased risk of money laundering in investment life insurance products results mainly from the possibility of investment by clients in the form of one-off extraordinary deposits or recurring deposits, as well as the possibility of partial surrenders and redemptions. These products are primarily linked to the investment component of the contract. On the other hand, there is a low ML/FT risk in term life insurance, which is aimed at covering classical insurance risk (death, survival) and is not linked to investments.

In the case of investment life insurance, the procedure for concluding contracts, including the identification of the client as well as the verification of the origin of the funds, is identical to the procedure used by insurance companies when concluding other life insurance contracts, i.e. these clients are treated in the same way, despite the higher risk of laundering.

In the Czech Republic, insurance premiums are usually paid into a bank account or by postal order. Premiums can be paid in cash when taking out insurance only for certain life and non-life insurance products (e.g. endowment life insurance, travel insurance, accident insurance, compulsory contractual insurance (hereinafter referred to as "Compulsory

Contractual Insurance"), whereas premiums received in cash are usually considered to be premiums collected on collection slips and premiums paid through a cash register at the insurance company's point of sale (these are mostly small amounts). The amount of cash acceptance of insurance premiums in the Slovak Republic is completely insignificant in relation to the total amount of premiums received.

Insurance companies pay claims exclusively to a bank account or by postal order to the address of the beneficiary.

Insurance companies domiciled in the Slovak Republic provide insurance products across borders within the EU only to a limited extent. These are mainly non-life insurance products (e.g. property insurance, travel insurance, liability insurance, parcel insurance and others).

Slovak law does not allow anonymous use of products. The internal regulations and procedures of insurance companies in accordance with the AML Act provide for the obligation to refuse to enter into a business relationship in the event that they refuse to identify themselves when entering into an insurance contract or refuse to declare on whose behalf they are acting. Insurance companies follow the same procedure in the case of insufficient identification of the person entitled to payment of the insurance benefit, i.e. the beneficiary of the insurance contract must always be known.

It is possible to conclude insurance contracts in an impersonal form for certain types of products, in particular non-life insurance products (e.g. travel insurance, accident insurance, compulsory contractual insurance, property insurance, etc.). The non-personal form of taking out insurance is considered to be online insurance via the internet, text message insurance, call centre (insurance taken out via the telephone services department), direct mail and insurance products taken out via selected financial intermediaries.

According to the European Commission's **Multinational Risk Assessment**, ML/FT risks in the insurance industry can be found in life insurance and annuity products. These products allow the client to insert funds into the financial system and potentially disguise their illicit origin or finance illegal activities. Relevant risk scenarios are typically focused on investment products in life insurance (and not on death benefit products). Risks may arise from or be manifested by one or more of the following factors:

1. The insurer accepts payment of the premium in cash.
2. The insurer shall refund the premium on cancellation or termination of the policy before maturity to an account other than the original source of funding.
3. The insurer does not perform due diligence on KYC in general and the source of investments in particular.
4. The insurer sells transferable policies (which are not ordinary).
5. Investment transactions include trusts, mandate holders, etc.
6. The insurer sells bespoke products where the investor dictates the underlying investment or portfolio composition.
7. An insurer may initially sell an investment contract at a low value; where the investor has the option to make another large investment without further KYC checks.

Terrorism financing risk exists for items 2, 4 and 6 above for direct and indirect financing of terrorist operations.

The risk of ML exists in all of the above cases. The perpetrators would use risk scenarios (1, 6, and 7) for placement, (2 and 4) for layering, and (2, 4, 6, and 7) for integrating.

There were no cases of ML in the insurance sector in the Slovak Republic during the reporting period. There have been cases where insurance products have been used in fraudulent activities, especially in non-life insurance (accident insurance, compulsory contractual insurance, property insurance, etc.). The vast majority of these are mainly bogus motor insurance claims. As regards the reputation of insurance companies in terms of involvement in financial crimes, including tax evasion, it can be assessed that so far no insurance company has been recorded in Slovakia that has been associated with involvement in financial crimes, including tax evasion.

c) ML/FT risk assessment of business relationships

A high-risk business relationship is a business relationship with a client that has any of the following risk factors:

a) the country of origin of the client, the country of origin of the owner of the client-entrepreneur, the country of origin of the founder of the client-non-entrepreneur, is included in the FATF's list of countries where measures against ML/FT are not sufficiently applied or in the list of countries that are considered to be tax havens,
b) the inclusion of the client, the founder of the client - non-entrepreneur, the owner of the client - entrepreneur, or the person with whom the client concludes business on the list of persons and movements against whom sanction measures are applied in accordance with specific legislation,
c) the client is on the list of PEPs,
d) the origin of the client's funds is unclear or the client declares the origin of the funds to be, e.g. a cash win in a casino, receipt of a cash gift, acquisition of an inheritance, etc.,
e) facts giving rise to suspicion that the client is not acting on his/her own behalf or that he/she is disguising that he/she is carrying out the instructions of a third party,
f) the manner of execution of the trade is unusual; or
g) a fact giving rise to suspicion that the client is carrying out an UT.

Vulnerability assessment and vulnerabilities

In the insurance sector, on the basis of the input data, **the risk score was set at 0.34 - low risk.** This means that the risk of ML in this area is present, but to a limited extent, taking into account the size of the insurance sector within the financial market, the nature of the insurance products, the potential clients, the sales channels, as well as the sufficient regulation of the insurance sector.

The identified low risk in the insurance sector is also a result of the application of simplified due diligence within the meaning of Section 11 of the AML Act by insurance companies which, subject to compliance with the conditions set out in the AML Act, is widely

used by insurance companies when concluding the majority of insurance contracts in life insurance. However, the use of the simplified due diligence in relation to the client does not exempt the liable person from monitoring the transactions and business relationships sufficiently so that unusual business operations can be detected and reported to the FIU SR without undue delay.

The slight decrease in the risk score compared to the previous NRA 1 may be a reflection of the adoption of the NBS internal regulation on risk-based supervision in March 2018 and the subsequent increase in the frequency of remote supervision of insurance companies in the area of AML in the form of questionnaires, which are sent to insurers and evaluated every 2 years. At the same time, the number of on-site supervisions carried out by the NBS, which focused on the control of insurance companies in fulfilling and complying with the obligations laid down by the AML Act, has been increased since 2018, with 5 thematic supervisions focused on the supervision of AML being carried out.

The issuance of the Methodological Guideline of the National Bank of Slovakia's Financial Market Supervision Units No. 5/2019 of 9 May 2019, which, among other things, eliminated shortcomings resulting from application practice, may also have a positive impact on the risk score. In order to guide insurance companies in their risk assessment, the ESAs Joint Committee's Joint Guidance (JC 2017 37) on simplified due diligence and enhanced customer due diligence and on factors that credit institutions and financial institutions should consider when assessing AML risk with individual business relationships and occasional transactions has been implemented in Annex 1.

The greatest risk of ML/FT in the insurance sector is in the case of clients with unclear ownership structure and if the legal entity as a potential client cannot sufficiently demonstrate from which sources he/she has obtained the funds he/she invests in specific products.

Funds related to insurance contracts (insurance premiums, insurance benefit payments) are directed from clients' accounts held in other financial institutions, mainly in Slovak banks, or they are cash payments made through trading points of Slovak banks and offices of the Slovak Post, a.s., while all these entities are liable persons who clearly have to comply with all the obligations arising from the AML Act.

Based on the above, it follows that the banking sector has the most important ML/TF protection function. The banking system should prevent the entry of illicit funds into the financial system by rigorously fulfilling the obligations of banks as liable persons under the AML law.

In general, there are no perceived particular risks of ML/FT in the insurance sector, as long as client funds are received or sent to the institution exclusively by means of wire transfers and the standard measures on fund transfers are applied to these (Section 20a, Section 10, Section 12, Section 14 of the AML Law).

Proposal for measures to mitigate identified risks and vulnerabilities

In order to ensure sufficient enforceability of the fulfilment of AML obligations by insurance companies, it is necessary to create a sub-legislative standard for the NBS as a

supervisory authority, in consultation with the Ministry of the Interior of the Slovak Republic, which specifies in more detail the content of the obligations of insurance companies as liable persons arising from the AML Act.

There is also a need for a sub-legislative standard to make it mandatory to conduct periodic internal or external audits on AML. Also ensure that first contact employees (or financial intermediaries) have access to information about the client and their trades that has been obtained through prior due diligence on the client (e.g. business and risk profile - KYC, client's risk group classification).

It is also necessary to recommend that insurance companies (or the association - SLASPO), once the legal requirements have been met, provide their own access to bank account information via the automated bank account retrieval system (crif).

From the point of view of ensuring the prevention of ML/FT, training of insurance companies' employees in the field of AML is an important component, and therefore it is necessary to increase the number of training events organised by the NBS and the FIU SR with the strong cooperation of the Association of Insurance Companies, as well as the number of working meetings with supervised entities aimed at resolving uncertainties arising from the application practice. It is also necessary for insurance companies to make greater use of the institute of qualified application, which is designed to deal with specific situations arising in the practical application of the AML Act, through the FIU SR website.

It is also necessary to increase the number of AML-oriented supervisions/inspections in insurance companies. This implies, especially in the case of the FIU SR, the need to increase resources and trained employees and to relieve the Control of Liable Persons Department of work activities not directly related to the performance of controls.

As no sanctions were imposed during the period under review as part of supervision/inspection, which could not have any deterrent effect, it is therefore necessary to tighten the sanctioning by imposing monetary fines for individual breaches of AML legislation in accordance with Government Resolution No. 207 of 7 May 2019.

It is also necessary to ensure that insurance companies**:**

- diligently exercise due diligence in relation to the client (Section 10(4), Section 20a of the AML Act), including identifying the origin of funds in relation to the risk of ML, the BO and the assessment of individual trades (high volumes of funds),
- when assessing trades, ascertain the origin of the funds entering the system,
- consistently identify the reason for the unusualness of individual trades that are the subject of UT reports, so that the unusualness is not focused solely on the exit of funds (underwriting, termination of insurance) from the insurance segment,
- all information from the basic due diligence already carried out was included in the UT reports,
- they also focused on continuous monitoring of the business relationship, as well as on a comprehensive assessment of individual transactions (extremely high deposits) using the KYC principle.

THE RETIREMENT SAVINGS SECTOR

General information on the retirement savings sector, consisting of the Old-Age Pension Saving and the Supplementary Retirement Savings.

Old-age pension savings (hereinafter also referred to as "Old-age pension savings"**)** or the so-called **second pillar of the pension system** is a savings system in Slovakia which, together with pension insurance (i.e. the first pillar of the pension system), is supposed to provide an income to the saver in old age or to the survivors in the event of the death of the saver. It is saving on the personal pension account of the saver, which on the basis of Act No. 43/2004 Coll. on old-age pension scheme is carried out by pension management companies since 1 January 2005 (hereinafter referred to as the "Act on old-age pension scheme"), on the basis of a permit issued by the National Bank of Social Security (NBS) and is subject to its control activities.

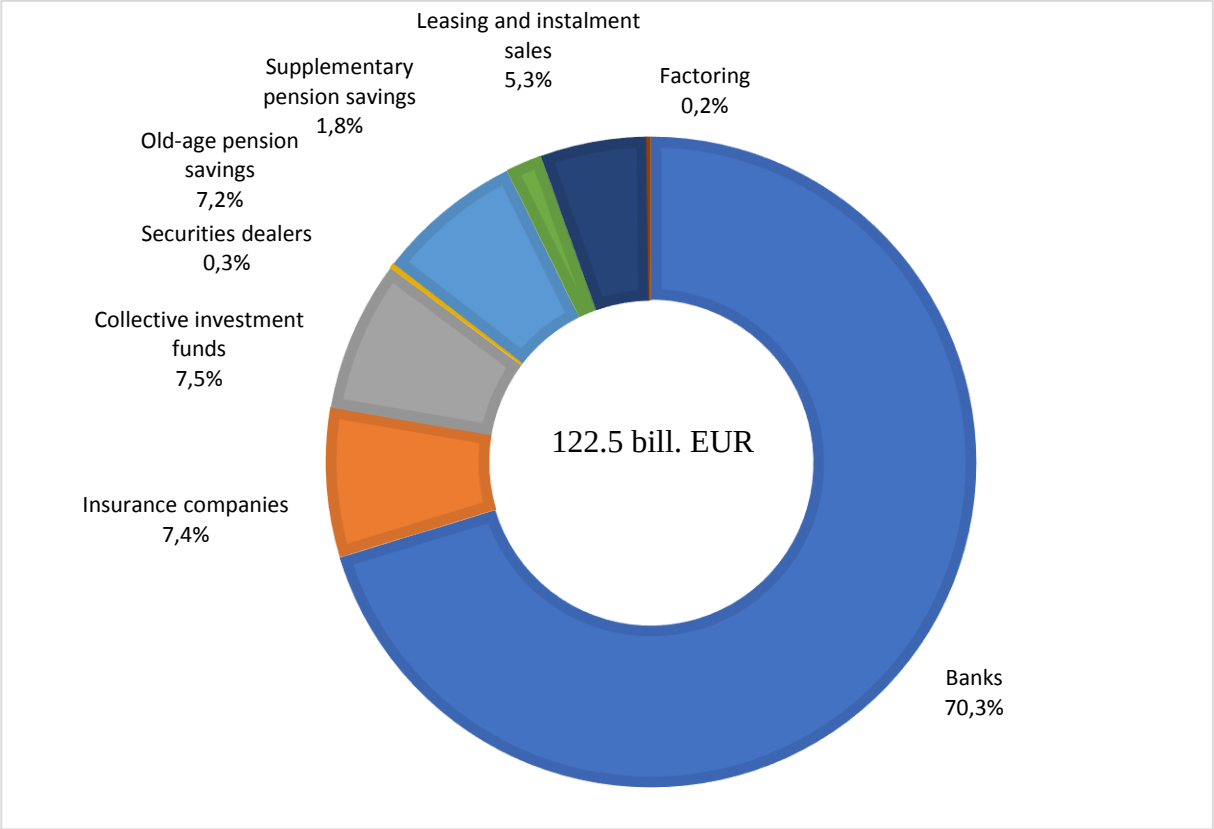
Supplementary pension savings (hereinafter also Supplementary pension savings) or the so-called **third pillar of the pension system** is a contributory defined contribution insurance funded through capitalisation, which is administered by supplementary pension companies. Its purpose is to enable participants to receive a supplementary pension income in old age and a supplementary pension income in the event of termination of so-called hazardous work. Supplementary pension savings are carried out by supplementary pension companies pursuant to Act No. 650/2004 Coll. on Supplementary Pension Income (hereinafter referred to as the "Supplementary Pension Income Act"), on the basis of a permit granted by the NBS and are its regulated entities of the financial market. Both old-age pension savings and Supplementary pension savings are financial market entities that fall within the portfolio of supervised entities of the National Bank of Slovakia in the area of AML.

In the period under review, there were active in pension savings on the Slovak financial market:

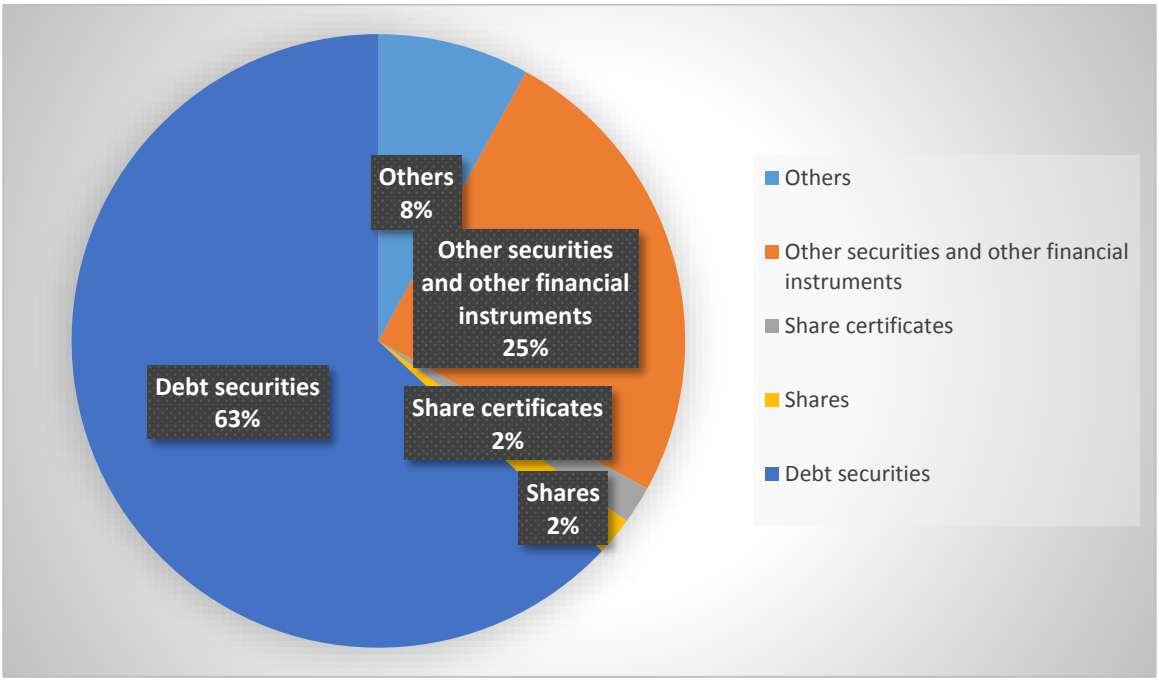
- **5 pension management companies** at the end of 2019 (6 at the beginning - there was a merger of two companies), which together **managed 17 pension funds** at the end of the assessment period (21 funds at the beginning of the assessment period);
- 4 supplementary pension companies managing a total of 17 supplementary pension funds

  At the end of the reporting period, pension sector companies accounted for 9% of the financial market in terms of the size of assets under management of financial market entities

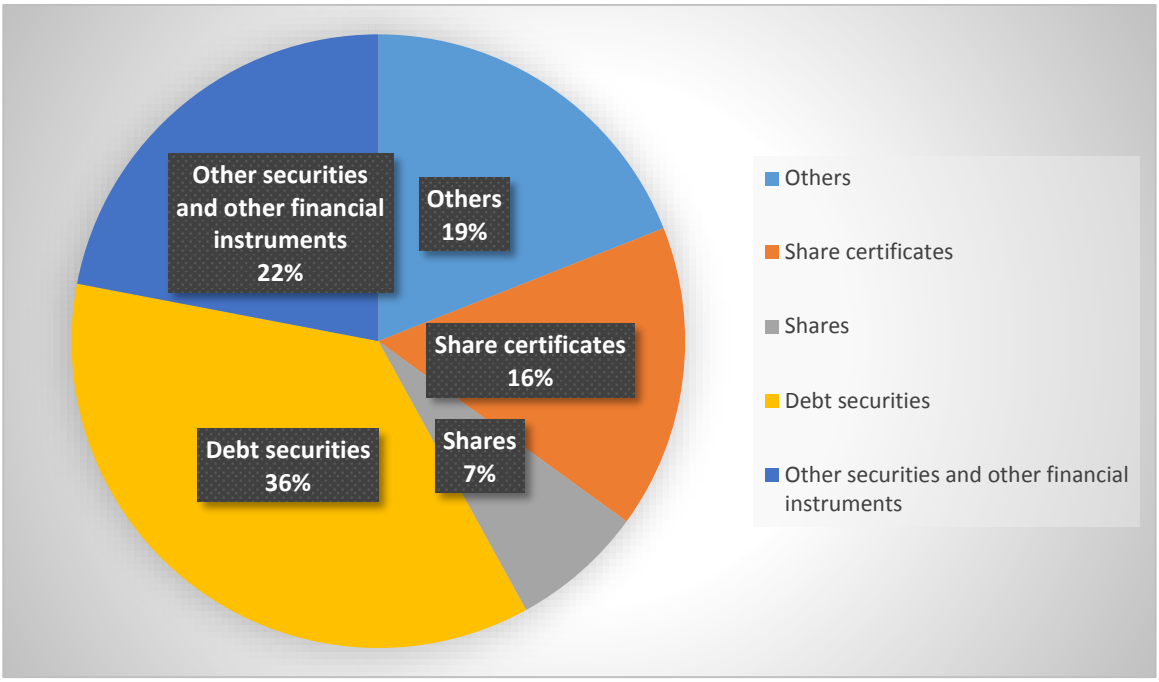
The total net assets under management at the end of the assessment period amounted to **EUR 9,324,469,611** in the old-age pension savings scheme and **EUR 2,373,220,090** in the supplementary pension savings scheme



Distribution of Old-age pension saving assets at the end of the assessment period



Distribution of Supplementary retirement saving assets at the end of the assessment period



Conclusions from the previous NRA

Based on the analysis of the information submitted in the previous assessment period 2011-2015, the steady state risk score was 0.17, i.e. low, which meant that the risk of ML in the sector was almost minimal.

One of the identified shortcomings was the absence of secondary legislation in the form of an AML measure, where the duties and tasks of liable persons operating on the financial market, imposed by the AML Act, would be specified in more detail. However, during the period under review, there was still no enabling provision in the AML Act to issue this legal standard.

From the information presented during NRA 1, it was noted that the number of UTs reported at 6 was low, again underlining the finding of a lower risk pension sector. In general, the analysis of the UT reports showed that the vast majority of them were evaluated within the discretion of the pension management companies as regulated in their own activity programmes. An important role in the prevention and fight against ML/FT is played by the function of monitoring compliance with the obligations imposed in this area. The pension savings sector is supervised in the area of AML by both the NBS and the FIU SR. The documents evaluated in the framework of NRA1 showed that 15 comprehensive supervisions were carried out by the NBS, which also assessed the AML area, where no deficiencies were found. No supervision was carried out by the FIU SR during the period under review. No sanctions have been imposed in the retirement savings sector in this area. Within the examined area, it was found that pension companies used manual risk adjustment of the client from the AML/CFT point of view, furthermore, the number of clients belonging to the higher risk virtucategory was very low and also the automatic reclassification of clients for whom unusual behaviour was identified to a higher risk level was not always taken into account.

Due to the fact that pension management companies do not deal with cash and all payments credited to the accounts held by them are transferred either from the Social Insurance

Institution or from employers, which are always transferred from banking institutions, the risk of ML in this sector is eliminated to a minimum.

Following the NRA1 assessment, the retirement savings sector was considered not to be associated with any involvement in crimes of this nature, including tax evasion, in terms of the institutions' reputation for involvement in financial crime.

Process risk and vulnerability analysis

AML/CFT legislation for the pensions sector

The Slovak legal system provides a comprehensive set of laws and legal norms regulating preventive measures against AML and FT, as well as the exercise of control and supervision over entities carrying out business activities in the pension savings sector. In addition to Slovak legally binding regulations in the area of old-age pension savings, the regulation of the activities of entities in the pension savings sector is also influenced by EU legally binding acts, international standards in the area of supplementary savings and, last but not least, by the knowledge, practical experience and generalised results from the NBS supervision and application practice.

The primary legal regulation of the individual institutes and obligations in the field of prevention of ML/FT is the AML Act. It is the basic legal framework governing the obligation to apply a risk-based approach to clients.

Pension management companies, as liable persons, must have an overview of the potential risks associated with a particular client. On the basis of the information thus obtained, they are obliged to determine the scope of due diligence and, where necessary, to apply enhanced due diligence measures, which is exceptional in the sector.

At the same time, the retirement savings sector is regulated by the Act on Old-age pension scheme and the Act on Supplementary retirement scheme, which constitute the general legislation in this sector setting out the rights and obligations of entities operating in the retirement savings sector, while in the case of persons managing a company or performing key functions, both the Act on Old-age pension scheme and the Act on Supplementary retirement scheme presuppose the fulfilment of the requirements of professional competence and credibility. The condition of credibility of employees of pension companies is normally regulated by the internal rules of the companies, with most of them requiring, in order to prove the credibility of employees, a criminal record statement or other necessary documents, including the submission of an employment reference from a previous employer or the results of their own investigations.

The legislation on the imposition of criminal sanctions is comprehensive and sufficient. However, in application practice, no such sanctions were imposed in the period under review, given the deficiencies identified and their low severity.

The comprehensiveness of the above-mentioned legal regulation of the activities of entities of the pension sector is also supplemented by detailed explanations on the fulfilment of

the obligations arising from the legislation elaborated in the form of methodological guidance of the NBS[88] and legal opinions of the NBS in the given area.

However, in the assessment period (2016-2019), there was still no uniform sub-legislative norm (e.g. in the form of a decree or a measure) in the legal framework of AML regulation, which would specify in more detail the individual areas and the content of the obligations for pension companies, which are generally regulated in the AML Act.

This deficiency has been remedied by amending the AML Act with effect from 1 November 2020 by adding a new paragraph 5 to Section 20, which empowers the NBS to issue a generally binding legal regulation after consultation with the Ministry of Interior.

The currently effective Methodological Guideline of the NBS has only a recommendatory and non-binding character with lower legal force of its application as well as of the enforcement of the performances resulting from it.

Internal AML/CFT regulations

The rules of conduct for employees of entities in the retirement savings sector are, by default, laid down in internal rules, which are regularly updated and accessible to all employees via the internal IT network. They are generally aimed at preventing conflicts of interest, insider trading or insider abuse. Internal regulations also have mechanisms in place to protect employees from the negative consequences and risks of reporting UT.

As in all financial institutions operating on the Slovak financial market, the responsibility for the overall protection of companies in the area of AML/CFT rests with the Board of Directors, whose direct management responsibility lies with a designated person. In specific cases, it is under the direct management responsibility of the CEO.

The designated person is responsible for the practical implementation of the AML/CFT measures. The independence of the function is due to its separation from operational and business activities, including the unrestricted right to communicate with employees and to access information relevant to the exercise of his/her rights and duties. In most pension management companies; the position of AML officer is part of the key compliance function or is included in a senior staff position. In this area, it can be concluded that, given the size of the sector as well as the activities carried out and the resulting risk of ML in the area of pensions, the staff resources in the companies are sufficient.

The basic internal regulation for the methodical provision of AML in pension management companies is the Own Anti-Money Laundering Programme, which is intended for all employees. The overall level of staff knowledge and understanding of AML/CFT obligations is sufficiently high.

Effectiveness of supervisory practices and methods (NBS and FIU SR)

Supervision over the fulfilment of the obligations of pension companies as liable persons under the AML Act is carried out by the NBS and the FIU SR. AML screening is

carried out by the NBS as a supervisor as part of comprehensive supervision (or post-supervision) or separately as a thematic supervision. **During the period under review**, **two comprehensive supervisions were carried out,** which included a review of the protection ML of the proceeds of crime. Supervision in the old-age pension savings sector was carried out with no deficiencies or findings in this area.

In the supplementary pension savings sector, one comprehensive supervision was carried out during the period under review, where two deficiencies with a lower severity and one finding with a higher severity were identified in the area of AML.

Deficiencies of a lower severity were as follows in the area of non-compliance with internal rules:

- the supervised entity, i.e. the liable person under the AML Act, has not properly developed and updated his/her own activity programme, in particular in the area of the overview of the forms of UT according to the subject of his/her activity, the method of risk assessment and management and the content and timetable of employees training have not been defined,
- the 'Report on ML and proceeds of crime activities', which should have been submitted to the statutory body at least once a year, was not submitted and thus implemented as part of the on-the-spot supervision for the period under review.

The deficiencies with a higher severity level were as follows:

- there was insufficient training of the company's employees, aimed at familiarising them with the own activity programme (hereinafter referred to as "the programme"), at least once per calendar year and always before the employee is assigned to a job where he/she will perform tasks under the AML Act, which resulted in a breach of the obligation defined in the company's internal regulations, and thus of a provision of a specific legal norm in the field of supplementary pension savings (Section 28(2) of the AML Act) - the obligation to draw up and comply with the internal regulations,
- the company failed to submit, for the on-site supervision period under review, a record of the AML training that it was required to and should have conducted annually and prior to assigning an employee to the job.

Thematic supervisions focusing exclusively on AML were not carried out in the pension savings entities in the period under review, nor was there supervision by the FIU SR or integrated supervision by the two competent institutions in the sector.

On the basis of all the findings as well as the assessment of the procedural aspects related to the performance of activities and internal processes of individual pension saving entities, the following potential vulnerabilities were identified:

- insufficient/inconsistent application of legislation - AML Act,
- Absence of mandatory elements in the Programme of Own Activities, more effective implementation of mandatory training as well as post-testing of employees,
  lower use of automated UT monitoring systems
  (dominated by manual),

- lower use of automated systems for monitoring PEPs (predominantly manual),
- low number of inspections carried out by the competent authorities of the FIU SR/NBS and no sanctions were imposed for breaches of the AML Act.
  Initial inspections - permitting procedures prior consents, notification obligations

The NBS, as a competent supervisory authority, has sufficient powers under the comprehensive legal and regulatory framework to carry out control activities also in the framework of the authorisation procedure, the procedure for granting prior consent to a specific legal transaction. At the same time, it fully applies its control mechanism to control all reporting obligations on the part of supervised entities. Pension companies are obliged, like all entities on the financial market subject to the supervision of the NBS, to notify without undue delay any changes that should occur or have occurred in the management of the company or in its professional activities.

Credibility and integrity of employees in the retirement savings sector

Under the legislation in force and in effect, a natural entity is a person of integrity who has not been finally convicted of a deliberate criminal offence or of an offence committed in connection with the performance of his or her duties. Integrity is demonstrated by a criminal record certificate no older than three months, which is required of all new recruits in all companies and, where applicable, whenever key positions are filled. The condition of integrity and trustworthiness of employees is normally regulated by pension companies in their internal regulations, work rules, and they also require proof of such integrity and trustworthiness, e.g. by declaration of honour or personal interview, references from previous employment, as well as information obtained from public sources and also in the World Check.

In the case of persons proposed as members of the Board of Directors, members of the Supervisory Board, proxies, senior employees under the direct management responsibility of the Board of Directors, key positions, senior management, integrity, credibility and professional competence are also assessed as part of the authorisation procedure conducted by the NBS.

In order to prevent conflicts of interest, insider trading or misuse of inside information, pension companies have rules of conduct for their employees laid down in internal rules, which are generally accessible via an internal intranet network.

At the same time, in accordance with Section 20(2)(i) of the AML Act, companies in the sector have a mechanism in place to protect their employees from the negative consequences and risks that may arise for employees when reporting an UT.

During the period under review, no suspicions of intentional criminal offences of a pecuniary nature committed by their employees were recorded by pension management companies.

Pension management companies also do not record any employees who have violated internal rules to prevent conflicts of interest, insider trading or misuse of confidential

information, except for one case of unauthorized interference in the personal pension accounts of their family members by hacking into the company's IT system, where the employment relationship with the employee was terminated and the subsequent settlement in the form of compensation for damages caused.

No prosecution has been initiated against the employee by entities operating in the retirement savings sector in relation to the breach of AML/CFT obligations.

Staff knowledge of AML/CFT in the retirement savings sector

The most important internal regulation in this area is the Companies' Own Activities Programme ("the Programme"), which, together with other internal regulations governing training, the system of internal education and training, forms the legal framework for employee training in the field of AML.

The system of employee training generally consists of a mandatory initial training for new employees and subsequently recurrent training once a year for the purpose of reviewing knowledge, training in the form of e-learning, or personal training with the participation of AML specialists and, last but not least, external training of responsible persons organised by the competent authorities (e.g. also the NBS).

The overall level of employees' knowledge of AML obligations in the retirement savings sector (in particular the obligation to report UTs, the ability to assess the riskiness of client behaviour, situations) was rated by the companies themselves in the questionnaires sent with a score of 2 (on a numerical scale of 1 - 5, the best - 1 and the worst -5). The above assessment reflects the knowledge of the employees of companies operating in the retirement savings sector, but also takes into account minor shortcomings in the field, which have been identified in particular in the categorisation of clients within risk classes or in the monitoring of PEPs.

Organisation of compliance in the retirement savings sector

Companies operating in the retirement savings sector have a clearly defined division of responsibilities and accountability for AML in their organisational structure. Comprehensive AML/CFT protection of pension management companies are the responsibility of the board of directors (or one of its members precisely defined in the organisational regulations or in the articles of association of the companies) and the practical performance of the activity is the responsibility of a designated person who is under the direct management responsibility of the board of directors or the chief executive officer, as the case may be. In its absence, its cover shall be provided by a competent person. The compliance function is materially and competently ensured in pension savings institutions so that it is independent and can be carried out properly and with due professional diligence. As pension management companies are financial market entities with a lower number of employees, the subject activities and the AML agenda in the monitored period were implemented by one full-time employee as a responsible person in the vast majority and in some of them the organisational provision of the AML agenda is implemented within a separate department or as part of the legal and compliance department.

Unusual transactions in the retirement savings sector

The general forms of the UT are explicitly set out in the basic legal norm regulating the AML area (Section 4(2) of the AML Act). The legislation governing old-age pension savings and supplementary pension savings does not regulate or specify unusual business operations, as they are very rare in this area.

Pension companies, as liable persons under Section 14(1) of the AML Act, are obliged to assess whether the business being prepared or carried out is unusual. The assessment of the unusualness of transactions, the method of conducting the assessment, the timing of the assessment as well as the evaluation or comparison with other UTs as well as the follow-up procedure are regulated by the companies in the Programme. From the submitted questionnaires it is possible to generalise the basic aspect of the assessment of the UT in the field of retirement savings and that is the **riskiness of the client**, since the nature of the transaction, the content as well as the method are clearly defined by the law on the old-age pension scheme as well as the supplementary retirement scheme and there is no need to assess the nature of the transaction.

Forms of UT in the retirement savings sector:

- refusal to identify the client when concluding the -age pension savings scheme/ supplementary pension savings scheme contract,
- disproportionately high extraordinary deposits into a personal pension account in the supplementary pension savings sector, where such operations (extraordinary deposits) are permitted by law,
- high extraordinary contributions by a supplementary pension savings participant if he/she is both an employee and a director in his/her own legal entity (s.r.o. (Ltd.)),
- an unusually high contribution to a client's contract who was already a beneficiary at the time it was sent (he/she had become eligible to apply for pension payments),
- the client is from a country at risk (Iran),
- sending a large contribution to a contract/account, which the client subsequently asked to be refunded, but to a different account, claiming that it was a mistake.

Method of conducting the assessment of UT in the pension sector:

Due to the fact that companies operating and carrying out both old-age pension and supplementary retirement pension savings are part of large financial groups, they are mostly provided with automated monitoring of UT through their internal group systems, but in some of them the assessment of UT is also carried out in a semi-automated or manual way, especially in second pillar companies (old-age pension saving scheme), where ML is exceptional and, given the number of UT, this is sufficient.

On the basis of the above, there is little likelihood of ML in the activities of both old-age pension and supplementary retirement saving entities.

This is evidenced by the fact that in the period under review there were a total of 9 UT reports in the supplementary retirement savings sector and 0 UT reports in the old-age pension savings sector.

Old-age pension savings scheme and supplementary retirement savings scheme

Year	Accepted		Retrieved from				
	Total UT	of this from Old-age pension savings scheme and supplementary retirement savings scheme	National Criminal Agency (NAKA)	RH PF, DH PF	FD SR	FIU SR	DTB
2016	3,297	0	0	0	0	0	0
2017	2,636	1 (Supplementary retirement saving)	0	1 (Sec. 197/1d)	0	0	0
2018	2,509	6 (5 Supplementary retirement saving, 1 Old-age pension saving)	2	1	0	0	3
2019	2,576	2 (Supplementary retirement saving)	0	1 (Sirene)	0	1	0

The analysis of the reports revealed that in some cases of supplementary retirement savings scheme and old-age pension savings scheme reports, the unusual nature of the transaction was incorrectly identified and justified by the "mere existence" of an international arrest warrant issued by the law enforcement authorities against the liable person's client, and in one case, the trade was also refused under Section 15 of the AML Act for the above reason.

Vulnerability and risk of the pension sector

The overall vulnerability of the pension sector in the conditions of the Slovak Republic, based on the assessment of the collected information and input data, has been determined in the framework of the first NRA at a low level - numerically expressed as 0.17 , which means that the risk of ML in this area is almost minimal.

In all phases of the ML process, banks and the banking system play a key role, as even in the area of pension savings, the funds coming into the system are transferred from the Social Insurance Institution or from the accounts of individual banking institutions.

Pension companies do not deal with cash as it is not possible to transfer contributions to both old-age and supplementary pension savings in the form of cash.

From an AML/CFT perspective, the retirement savings sector can be assessed as the least attractive compared to the banking sector for ML and TF.

AML/FT assessment of product/service risk and client risk in the sector

Old-age pension savings is an area where only one product is provided to clients, which is a pension product. The essence of this financial product is the accumulation and management of clients'/savers' assets by investing in the financial markets. Savers' funds represent

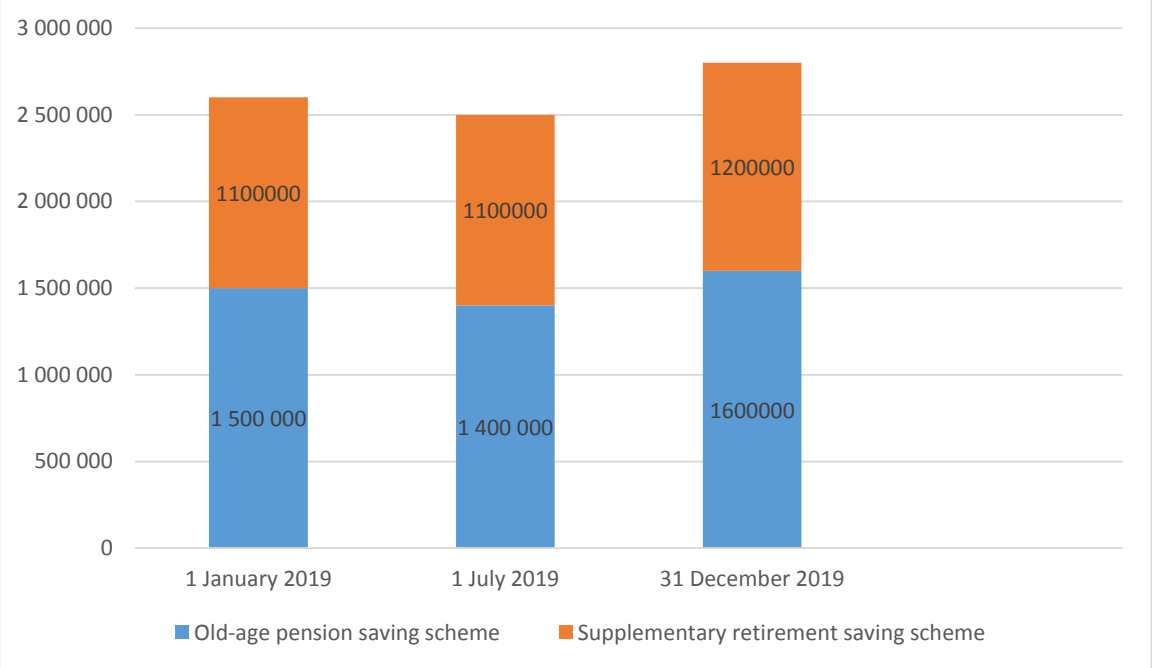
compulsory and voluntary contributions, which are managed by pension management companies and supplementary retirement companies. As mandatory contributions are sent directly from the accounts of the Social Insurance Institution and voluntary contributions of a minimum amount are sent exclusively from accounts held with other financial institutions, retirement savings are not a risky service from the point of view of the ML/FT.

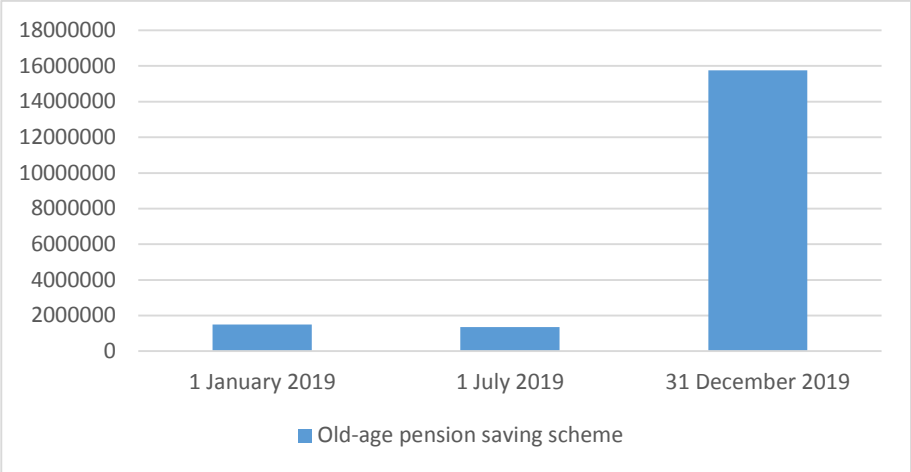
The risk is further minimised by the fact that the free disposal of funds is strictly limited by the old-age pension savings scheme Act and both compulsory and voluntary contributions credited to a personal pension account can only be used once the statutory conditions have been met.

Minimised risk also arises from the **client base in the sector itself**.

Clients/savers are exclusively natural entities - employees and self-employed persons registered in the territory of the Slovak Republic. Also, **the BO** that the liable persons under the AML Act are required to monitor are exclusively the clients/savers or their designated beneficiaries in the event of the death of the saver.

Evolution of old-age pension savings scheme savers/participants in the supplementary pension savings scheme at the end of the assessment period:





Supplementary retirement saving is also a financial service that consists in the accumulation and appreciation of funds in the personal pension accounts of individual clients/participants by supplementary pension companies. In this area of pensions, contributions are paid directly from the employer or paid directly to the client. However, even here the risk of ML is eliminated by the fact that contributions are not handled in cash but must be paid exclusively by bank transfer from the financial institution. At the same time, the disposal of the saved funds is limited by the accrual of a pensionable entitlement or by the statutory minimum saving period of ten years from the establishment of the contractual relationship.

On the basis of the above, there is little likelihood of ML in the activities of both old-age and supplementary pension saving entities.

Both retirement savings entities use predominantly an internal network to sell their products, but also an external network where retirement products are offered through financial intermediaries, either through independent financial agents, subordinate financial agents or tied financial agents. Representatives of the external network carry out simplified due diligence, consisting in the identification of the client and its subsequent verification when signing a contract on retirement pension savings or when signing a contract on supplementary pension savings.

However, it is the pension management companies that, on the basis of all available information (i.e. not only that obtained from contract management), determine the factors and thus the risk grades needed to categorise clients and then set the appropriate level of measures in relation to each category. They also determine the features necessary to identify the potential risk of laundering and unusual activities of client-savers/participants, (type and scope of diligence, including the assessment of transactions and the enforcement of measures under the AML Law). It should be noted that the **ultimate responsibility for exercising complete due diligence in relation to the client lies with the pension management companies (strict liability),** despite the fact that financial intermediaries are also classified as liable persons within the meaning of Section 5 of the AML Act.

In general, there are no perceived specific risks of ML/FT laundering in the retirement savings sector as the funds of clients - savers/participants are received or sent to the institution

exclusively by means of non-cash bank transfers and the standard measures on fund transfers are applied to these (Section 10, Section 12, Section 14 of the AML/CFT Act).

Voluntary contributions, which are paid outside the Social Insurance Institution, may represent a **slightly higher risk** in the context of old-age pension savings, but their average annual amount is EUR 100 per month.

Contributions in excess of contractually agreed repayments may also be made under supplementary pension savings, but there were no unusual transactions, either in terms of excessive amount or frequency, for any entity during the period under review. At the same time, it is not permitted to accept contributions from third parties in this area.

Vulnerability assessment and vulnerabilities

The assessment of the procedural aspects related to the performance of the activities and internal processes of the individual entities of the retirement savings sector, as well as of the supervisory/control bodies, did not identify significant vulnerabilities, as the findings of the first NRA were fully incorporated into the processes.

At the same time, based on the input data, the risk score was set at 0.15 - very low risk in the retirement savings sector, which means that the risk of ML in this area is present to a minimal extent.

The slight decrease in the risk score compared to the results of the previous NRA may be due to the improvement of the supervisory approach in the form of the adoption and subsequent application in the application practice of the internal regulation of the NBS on risk-based supervision, incorporation of risk factors into the programmes of pension companies in accordance with the Methodological Guideline of the NBS.

As already mentioned, a new NBS Methodological Guideline No. 6/2019 for the capital market area, binding also for pension companies, was issued in the area of regulation (13 May 2019), the aim of which was to further regulate and guide pension companies in fulfilling their obligations in the area of risk assessment. ESA's Joint Committee guidelines (JC 2017 37) on risk factors to be considered when assessing individual business relationships and AML transactions have been implemented in its content.

In general, no specific AML/CFT laundering risks have been identified in the retirement savings sector as it is a sector with a low potential for ML due to the nature of the retirement savings product, as the pay-out of funds is linked to retirement age and the operation of the product is linked to employment from the outset.

In the period under review, there were no cases of ML in the field of pension savings, both old-age (second pillar) and supplementary retirement savings (third pillar) in the Slovak Republic.

The aforementioned facts related to lower risk are also the reason why pension savings entities perform only simplified diligence in relation to clients within the meaning of Section

11 of the AML Act, in which identification and verification of each client's identification is carried out either by a financial agent, a first-contact employee or by the Social Insurance Institution.

Given the identified low risk of ML/TF, liable persons in this sector may carry out simplified due diligence in relation to a client, subject to the conditions set out in the AML Act. However, the use of the simplified due diligence in relation to a client does not exempt the liable person from monitoring trades and business relationships sufficiently so that UTs can be detected and reported to the FIU SR without undue delay.

Proposal for measures to mitigate identified risks and vulnerabilities

Across the financial sector, in order to ensure the enforceability of the obligations imposed by the AML Act, which need to be specified in a subordinate legal norm, it is necessary to issue a sub-legislative norm with the force of secondary legislation.

There is a need to ensure that regular internal and external audits are carried out on AML obligations imposed in a stronger piece of legislation such as the methodological guidance. Increase the number of thematic supervisions focused exclusively on AML by competent supervisory authorities.

In the area of prevention and education, it will be necessary to increase the number of educational events organised by both the NBS and the FIU SR, as well as the number of working meetings with supervised entities aimed at resolving uncertainties arising from application practice

12. CAPITAL MARKET SECTOR

THE NATURE AND OPERATIONAL METHODS OF ANALYSIS OF THE SECTOR VULNERABILITY ASSESSMENT MODEL

The analysis of the capital market sector vulnerability assessment model is developed in line with the World Bank's methodology that was used in the development of the 2016 NRA. The report shall include the following points and evaluation criteria:

1. Capital market as a segment of the financial market
2. AML/CFT legislation in the capital market sector
3. Capital market entities/licences/financial market shares
    3.1 Collective investment area - management company
    3.2 Securities market area - securities dealer
3.3 Stock exchange, central depository, national central depository
4. Questionnaire survey of entities in the capital market sector, analysis of the results of input variables
    A. AML Organization, Compliance in the capital market sector
    B. Integrity of employees in the capital market sector
    C. Employees training in the capital market sector
    D. Effectiveness of monitoring and reporting of UT in the capital market sector
    E. Client base profile - risk categorization of clients from AML perspective, client categorization, risk assessment and identification
    F. Products, business relations
    G. Emerging ML/FT risks

Information on the implementation of the conclusions of NRA 1

4.1 Summary of the questionnaire survey

5. Effectiveness of monitoring and reporting of UTs
6. Results of supervision (overview of weaknesses and strengths of supervision)

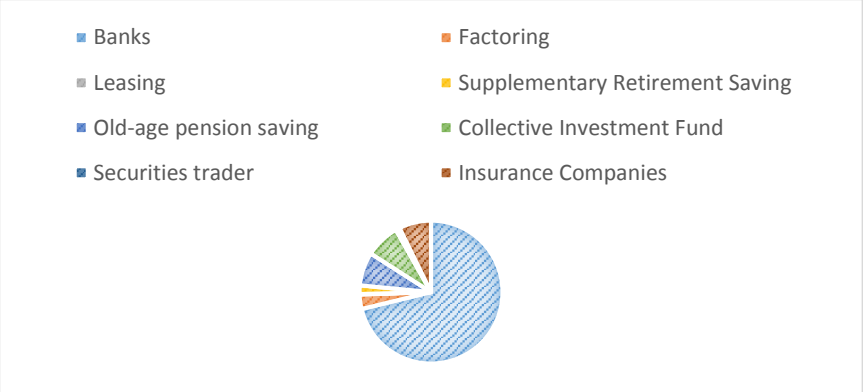
6.1 Availability and enforceability of administrative sanctions

7. Vulnerability assessment and risk analysis in individual institutions
    7.1. Transnational risk assessment by the European Commission
8. Identified weaknesses in the capital market sector and proposals for action

1. CAPITAL MARKET AS A SEGMENT OF THE FINANCIAL MARKET

One segment of the financial market is the capital market, i.e. the market for medium- and long-term capital used to finance investments. It is primarily in the form of freely tradable securities. The share of individual financial sectors in the assets of the entire financial market as of 31 December 2019 is shown in the following chart.

Chart 1 Share of financial market assets or assets under management



Source: NBS, Analysis of the Slovak Financial Sector 2019

The capital market in Slovakia does not sufficiently fulfil its basic economic functions, i.e. the creation, valuation and redistribution of free financial resources, and is thus not a place for the efficient meeting of capital and investment opportunities. This state of affairs has persisted for a long time. The capital market in Slovakia is one of the smallest functioning markets among the European Union countries. The minimal liquidity of the Slovak capital market and barriers to entry into this market result in Slovak investors preferring foreign markets that offer higher liquidity, lower fees and higher diversification of financial instruments. **This affects the vulnerability of the securities sector and the level of threat of ML/FT.**

The analysis of the vulnerability assessment of the capital market sector was focused on entities that have a minority position in the Slovak financial market.

2. AML/CFT REGULATION IN THE SECURITIES SECTOR

The basic legislation governing AML for all liable persons, including supervised entities in the CT sector, is the AML Act transposing Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of ML/FT, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. In order to implement the recommendations of the Moneyval Committee of the Council of Europe contained in the Fifth Evaluation Report on the implementation of measures against ML/FT in the Slovak Republic, as well as the revised recommendations of the FATF (Financial Action Task Force of the G7), it will be necessary to amend the AML Act.

The securities sector is also regulated in this area by Act No. 203/2011 Coll. on Collective Investment, as amended (hereinafter referred to as the "Act on Collective Investment"), Act No. 566/2001 Coll. on Securities and Investment Services and on Amendments and Supplements to Certain Acts (the Securities Act), as amended (hereinafter referred to as the "Act on Securities and Investment Services"), Act No. 429/2002 Coll. on the

Stock Exchange, as amended (hereinafter referred to as "Act on Stock Exchange"), Act No. 747/2004 Coll. on Financial Market Supervision and on Amendments and Additions to Certain Acts, as amended.

Since the legal regulation of this area is complex, as it is based not only on Slovak and European legally binding regulations, but also on international standards, on knowledge, practical experience gained in the exercise of supervision by the National Bank of Slovakia contained also in the Methodological Guideline of the Financial Market Supervision Unit of the National Bank of Slovakia of 13 May 2019 No. 6/2019 on protection against ML/FT in the activities of a securities dealer, a branch of a foreign securities dealer, a management company, a pension management company and a supplementary pension company.

The methodological guidance issued by the NBS is published on http://www.nbs.sk/_img/Documents/_Legislativa/_Vestnik/MU_6_2019.pdf

The methodological guidance issued by the FIU SR is published on www.minv.sk/?informacie-a-usmernenia-pre-povinne-osoby-a-zdruzenia-majetku

3. CAPITAL MARKET OPERATORS /LICENSES/ FINANCIAL MARKET SHARE

An important role in the AML/CFT system is also played by liable persons in the capital market sector, namely the ***asset management company, the securities dealer, the central securities depository and the stock exchange,*** which are liable persons within the meaning of the AML Act.

The aforementioned financial institutions operate in the capital market sector ***on the basis of a licence issued by the National Bank of Slovakia***. As a general rule, for all types of institutions, the following conditions must be demonstrated in order for authorisation to be granted:

- paid-up capital with a minimum amount,
- transparent and credible origin of the share capital or other financial resources (information on the origin, volume and composition of the funds to be contributed to the share capital),
- the suitability of the persons who will be qualifying shareholders of the institution and the clarity of the relationships of those persons with other persons, in particular the clarity of the shareholdings in the capital and voting rights,
- factual, personal and organisational prerequisites for the activity,
- the professional competence and credibility of the persons proposed as members of the board of directors, supervisory board, proxy and persons responsible for internal control (university degree, generally three years' experience in the financial market, aptitude and suitability test to prevent the granting of a licence to untrustworthy persons,
- he transparency of a group with close links, which includes a shareholder with a qualifying holding in the institution,

- the exercise of supervision is not hindered by close links within a group with close links,
- the ability of the founding shareholders to bridge any adverse financial situation,
- technical and organisational readiness to carry out the permitted activities (e.g. modification of statutes - separation and modification of powers and responsibilities of ML/FT protection institutions,
- requirements for institutions to have effective AML measures in place, including compliance manuals and the appointment of qualified employees for internal inspections/compliance, etc.

The area is strictly regulated and there is a comprehensive legal and regulatory framework in the legal order which provides the NBS with appropriate powers to carry out initial inspections, which are also part of the licensing procedure or other procedures for the granting of prior approval by the NBS. The institution is obliged to notify the NBS without undue delay of any changes in the persons managing it or in the persons proposed as members of the Board of Directors and senior employees under the direct management responsibility of the Board of Directors, including all information and documents necessary to assess whether the new natural entity meets the requirements of professional competence and credibility. The Capital Market Supervision Department competently assesses and evaluates the demonstration of compliance with the conditions laid down by specific regulations in individual proceedings, and also outside the proceedings if the subject of the review is reporting obligations.

On the basis of the assessment of the complete application, the annex to the application, as well as the material, personnel and organisational prerequisites in relation to the proposed scope of the given activity, the NBS shall decide whether to grant the applicant a permit or to reject the application or to grant the applicant a permit only partially. The conditions for the authorisation to carry out the activity in question must be fulfilled continuously during the period of validity of the authorisation in question.

3.1 COLLECTIVE INVESTMENT AREA - management company

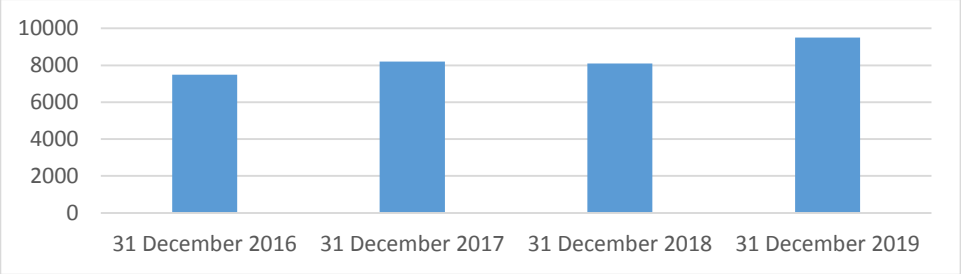
The rules of collective investment, the activity and operation of management companies and foreign management companies on the territory of the Slovak Republic, the creation and management of funds, the activity of the depositary, the cross-border distribution of units and securities of foreign collective investment entities, the protection of investors in collective investment, the activity of other persons involved in collective investment and supervision are regulated by the Act on Collective Investment.

On the financial market of the Slovak Republic, collective investment is represented by nine domestic management companies and one foreign management company, which had 96 domestic open-end funds under management as of 31 December 2019. Management companies create and manage the following categories of funds according to a set investment strategy: bond, equity, commingled, special real estate and other funds.

In terms of the development of the value of assets in collective investment funds in Slovakia between 2016 and 2019, a continuous increase compared to 2015 can be noted. Collective investment saw dynamic growth in 2017, with the net asset value of domestic and

foreign funds increasing by more than EUR 1 billion compared to 2016. The year 2018 can be assessed as less successful. Both domestic mutual funds and foreign collective investment entities contributed to the halt in the growth trend. Client inflows and rising asset prices drove record asset growth in the collective investment sector in 2019. As of 31 December 2019, the amount of assets in mutual funds reached € 9.6 billion. To illustrate the development of assets in mutual funds between 2016 and 2019, the following graphical representation can be given in thousands of EUR.

Chart 2 Assets in open-end mutual funds for the years 2016 to 2019 in thous. EUR



Source: the Slovak Association of Asset Management Companies

3.2 SECURITIES MARKET AREA - Securities dealer

The status of securities dealers, financial instruments, investment services, contractual relations, rules related to the activities of persons providing investment services and the activities of the central securities depository, certain relations related to the activities of other entities in the field of the financial market, as well as supervision, are regulated by the Act on Securities and Investment Services.

As of 31 December 2019, 22 non-bank securities dealers, 16 banks and branches of foreign banks and 2 asset management companies were active on the Slovak capital market as securities dealers.

With effect from 03 January 2018, new legislation in the area of regulation of investment services is in force in the Slovak Republic. Act No. 237/2017 Coll. amending the Act on Securities and Investment Services and amending certain acts transposed Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments amending Directive 2002/92/EC and Directive 2011/61/EU (the "Markets in financial instruments II Directive") into Slovak law. Markets in financial instruments II Directive, together with Regulation (EU) No. 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments amending Regulation (EU) No 648/2012 ("Markets in financial instruments Regulation"), collectively referred to as the Markets in financial instruments II Directive package, applies in particular to securities markets, investment intermediaries and trading venues.

The value of assets managed by entities licensed as securities dealers as of 31 December 2016 amounted to EUR 348 million. In 2017, the volume of assets under management by

securities dealers increased to EUR 403 million. The volume of trades executed by securities dealers decreased significantly in 2018. This decline was caused by a significant fall in bond trades. In 2019, the size of client assets managed by securities dealers increased to EUR 1.12 billion.

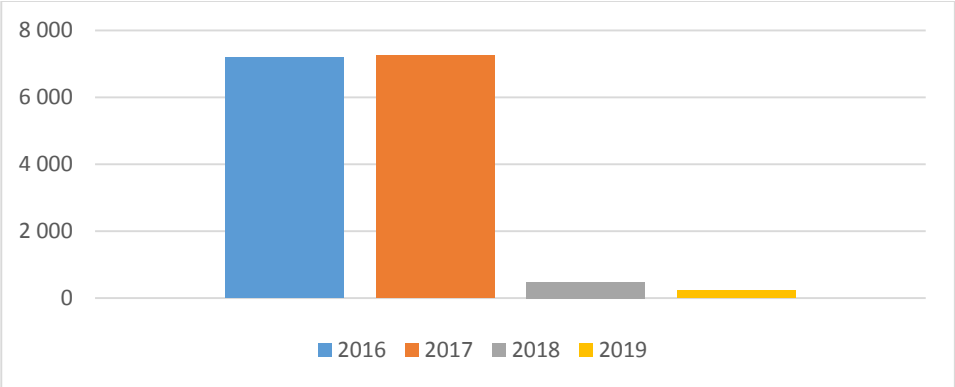
3.3 Stock exchange and central depository, national central depository

A. The Stock exchange is the entity authorised to organise the public securities market and related activities. This is a licensed and regulated activity governed by the Act on Stock Exchange. The stock exchange operates on a membership basis. Ordinary (common) and preference shares, units, corporate, bank and government bonds, mortgage bonds, municipal bonds can be traded on the stock exchange. ***As of 31 December 2019, the stock exchange had 11 full members.***

The volume of trading on the stock exchange had a significantly declining trend in the period under review. The year 2018 was a breakthrough year for the Stock Exchange due to the effectiveness of the Markets in financial instruments II Directive regulation, which brought changes in the system of services provided. It was the first year without government bond trades moving to the over-the-counter market, which brought an ultimate reduction in traded volumes, but the focus of the trades made shifted to the anonymous side. In 2019, the number of executed transactions on the stock exchange decreased by 40% and the volume of executed trades decreased by almost 50% compared to 2018.

As of 31 December 2019, 263 issues of securities (shares and bonds) were placed on the stock exchange market, including 21 issues on the listed main market, 22 issues on the listed parallel market and 220 issues on the regulated open market.

Chart 3 Development of the volume of trades executed on the stock exchange in million EUR



Source: Stock exchange yearbooks for 2016 to 2019

B. Centrálny depozitár cenných papierov SR, a.s. (Central Securities Depository of the Slovak Republic) operates under the Act on Securities and Investment Services on the basis of a licence granted by the NBS and its 100% shareholder is the stock exchange. The activities of the Central Securities Depository are also based on the membership principle and at the end of 2019 the Central Securities Depository had 26 participants (13 banks, 7 securities dealers, 3 foreign central depositories, Debt and liquidity management agencies, the National Bank of

Slovakia, National Securities Depository). A central depository is an institution providing in particular the registration of issues and holders of securities, the maintenance of securities holders' accounts, the change of securities holders, the establishment and maintenance of securities holders' accounts and other activities related to the activities of the Central Securities Depository. In the period under review, the Central Securities Depository saw increased issuer activity, an increase in revenues and a reduction in costs. As of 31 December 2019, a total of EUR 85,354 billion of book-entry securities had been credited to the accounts of holders, client accounts and custodian accounts. As of 31 December 2019, the Central Securities Depository maintained a register for 14,254 issuers of book-entry securities.

C. Národný centrálny depozitár cenných papierov, a. s. (National Securities Depository) operates on the member principle, i.e. it provides its basic services and products to capital market entities through its participants. In October 2016, the National Securities Depository became part of the list of member countries of ESMA, the European Securities and Markets Authority, which performs the functions of the European Union's financial regulatory agency. Since 2017, the National Securities Depository, as the only central depository in the Slovak Republic, has been providing services related to the registration of issues of shares of simple joint stock companies and related special rights of shareholders. The National Securities Depository is solely responsible for the registration of share issues for simple joint stock companies, and in 2019, the National Securities Depository registered share issues for 38 such companies. At the end of 2019, the National Securities Depository recorded a total of 180 issues of book-entry securities with a nominal value of EUR 686.3 million, representing a 68% year-on-year increase in terms of the number of cases. At the end of 2019, the National Securities Depository had a total of 159 lists of registered certificated shareholders on record.

QUESTIONNAIRE SURVEY, ANALYSIS OF INPUT VARIABLES

- As part of the preparation of the second round of the national risk assessment in the capital market sector, a questionnaire was sent to the entities, which was mainly aimed at identifying the following facts:
- organisational and methodological provision of AML in the company,
- condition of integrity of employees, prevention of conflicts of interest, insider trading, unauthorised trades; cases of whistleblowing, application of sanctions in case of non-compliance with internal regulations;
- the overall level of staff knowledge of AML obligations (types of AML training, overall level of staff knowledge of AML, knowledge tests and their evaluation, ensuring the availability of AML methodological materials and information for all staff), detection of deficiencies (staff failures) resulting from non-compliance with their AML obligations,
- detection of UTs (AML monitoring systems; parameters/criteria/scenarios; sanction list, PEP), forms of UTs and number of UTs captured and reported, procedure for reporting UTs);
- what type of due diligence the institution applies to the client in relation to the AML risk category and what actions (procedures) it applies within each type of due diligence; the process and verification of the BO,

- Emerging ML/FT risks, FT risk identification and management, FT risk management scenarios and models, crowdfunding project delivery, cum-ex schemes, VAPS and FinTech experience;
- implementation of conclusions after the 1st round of NRA (internal ML/FT risk assessments, new risks, measures, staffing, internal rules).

A total of 32 entities completed the questionnaire, including 22 securities dealers, 1 central securities depository, 1 national central securities depository, 1 stock exchange, 7 asset management companies. Based on feedback from reporting institutions, conclusions can be drawn on the following variables:

A. AML Organization, Compliance in the capital market sector;
B. Integrity of employees in the capital market sector;
C. Employees training in the capital market sector;
D. Effectiveness of monitoring and reporting of UT in the capital market sector;
E. Client base profile - risk categorization of clients from AML perspective, client categorization, risk assessment and identification;
F. Products, business relations;
G. Emerging ML/FT risks;
H. Feedback on the implementation of the conclusions of Round 1 of the NRA.

A. AML Organization, Compliance in the capital market sector

The organisational arrangement of AML within individual institutions is determined mainly by the Own Activity Programme and in most of the surveyed entities, the statutory body of the company is responsible for the overall protection of the financial institution against ML/FT and the implementation of the prevention concept. The designated person of the company (Compliance Officer) is responsible for the practical implementation of the activities and tasks arising from this programme.

The organisational arrangements for the AML agenda are generally as follows:

d) a separate organisational unit - the compliance department or the compliance & AML unit of the parent company (management companies),
e) a person responsible for the compliance function (Compliance Officer), possibly in cooperation with an external consultancy company,
f) the responsible official designated in the organisational structure and his/her designated representative.

Institutions shall ensure that the position of the Compliance Officer in the organisational structure of the company ensures his/her independence. The Compliance Officer is usually organised directly under the company's General Meeting of Shareholders at the level of the Supervisory Board, has precisely defined rights and duties through a system of internal regulations, as well as organisational and material support for the independent performance of his/her function, which he/she is obliged to carry out with professional diligence. The Compliance Officer does not have to be an employee of the company; the function of the Compliance Officer may be delegated to another natural or legal entity.

The responsibilities of the Compliance Officer include in particular:

a) ongoing preparation and updating of the programme and any other necessary regulations and procedures for ML/FT protection,
b) carrying out management and control tasks in the field of protection against ML/FT,
c) communication, cooperation and ongoing liaison with the FIU SR; including timely reporting of UTs,
d) the organisation and establishment of rules for the training of relevant employees of the company, including newly recruited employees,
e) analytical and advisory work in relation to the assessment and reporting of UTs by relevant staff in connection with the execution of client trades and business operations,
f) proposing amendments to AML regulations to the Company's Board of Directors in accordance with new legislation, facts and information,
g) preparation of the annual or semi-annual AML Performance Report, information for the Management Board and the Supervisory Board of the company.

In smaller companies, due to the low number of employees in the period under review, the activities and agenda in question were carried out by one full-time employee - the Compliance Officer or directly by the statutory body.

Within the stock exchange, the AML area is organised by the Exchange Inspection Department in cooperation with other departments, which informs the CEO of any violations of the AML rules. The Stock Exchange Inspection Department reports directly to the CEO.

Within the National Securities Depository, the company's statutory body is responsible for the overall AML protection of the company and the implementation of the prevention concept. The designated person responsible for the practical implementation of AML activities shall be the Compliance Manager.

Within the Central Securities Depository, the AML area is included in the organisational structure under the Compliance Department. The Company's Board of Directors is responsible for the overall implementation and compliance with AML requirements.

B. Integrity of employees in the capital market sector

Under the current legislation, a natural entity is presumed to be of integrity if he/she has not been finally convicted of a deliberate criminal offence or of an offence committed in connection with the performance of his/her duties. Every staff member shall prove his or her integrity on taking up employment by an extract from the criminal record no older than three months or, in the case of a foreigner, by a similar certificate of integrity issued by the competent authority of the State in which he or she has his or her permanent residence or by the authority of the State in which he or she habitually resides, which must be free of any criminal record. Some institutions require a declaration of honour that the person meets the conditions of integrity and trustworthiness set out in specific regulations. Some companies indicated in the questionnaire that they also require new hires to submit other documents such as a job reference,

references from previous employers, or obtain information from public sources or World Check.

The companies stated that other documents they use to verify the integrity of employees include data from the social insurance register or the credit register. Two companies indicated in the questionnaire survey that they also require a declaration of honour and a certificate from the local competent court that no criminal proceedings are pending against the employee.

Integrity checks are therefore an integral part of the selection process in any institution. In the process of recruiting new employees, the liable person in the securities sector follows the requirements of specific regulations and the condition of integrity of newly recruited employees is generally also stated in the Code of Ethics or in the Rules for Reporting Possible Violations of Internal and External Rules, the Insider Policy, the Conflict-of-Interest Policy or the Compliance Code, the Conflict-of-Interest Policy, as the case may be. In other cases, where the company's internal rules do not contain a specific regulation of the above-mentioned issues, the basic statutory framework is used.

In the case of persons nominated as members of the board of directors, proxies and senior staff under the direct management responsibility of the board of directors, senior management, the institution shall also verify compliance with the requirements for ***professional competence and integrity.*** Prevention and education in relation to employees against the occurrence of deficiencies/failures of employees resulting from non-compliance with their AML obligations is part of the regular annual AML training and on-boarding training for new employees.

A separate chapter is the protection of the employee from the negative consequences and risks arising from the reporting of UT. Liable persons are prohibited from applying any negative consequences to employees responsible for the application of AML/CFT procedures in the internal regulation governing the AML/CFT area. In doing so, the good faith of the employee shall be taken into account and presumed in case of doubt. Every employee of the institution, or persons acting for the liable person on the basis of a contract, are obliged by law to maintain the confidentiality of the reported UT and of the measures taken by the FIU SR in relation to the UT. No employee shall inform the client or other persons, including employees of the liable person, other than the responsible and designated person, of the UT report filed and related actions.

The obligation of confidentiality does not cease upon termination of the employment relationship or any other contractual relationship with the liable person. In the case of proceedings before law enforcement authorities, the confidentiality shall be waived for the liable person and his/her employee by the FIU SR. The duty of confidentiality shall be imposed on anyone who, in the performance of or in connection with the tasks of the FIU SR, becomes acquainted with information obtained on the basis of this Internal Regulation and the AML Law.

Most institutions implement in their internal policies the principle that no employee who reports a suspicion of misconduct, fraud or corruption in good faith will be subjected to any retaliation, even if the suspicion is not confirmed after investigation.

Accordingly, as far as external protection is concerned, it is in principle the case that compliance with the legal procedures (confidentiality obligation, prohibition to mention in the UT report any details of the employee who has detected the UT, etc.) sufficiently eliminates the risk of endangering the employee, e.g. from the client involved in the transaction.

During the period under review, no suspected intentional criminal offences of a pecuniary nature committed by staff members were recorded by the institutions contacted. However, two companies had 2 conflict of interest breaches during the period under review.

C. Employee training in the capital market sector

The most important internal regulation for this area is the Own Activity Programme regulating the issues defined in Article 20(2) of the AML Act, as well as other internal regulations intended for the training of employees in the AML area.

The staff training system generally consists of a mandatory induction training for new employees and a refresher training for employees - 1 time per year. Training takes the form of face-to-face training (personal training with the participation of AML specialists or external specialists), personal consultations, training sessions and e-learning, where specific cases from practice are usually presented. In the event of emergencies, an ad hoc meeting shall also be organised, as appropriate in scope and content, for the purpose of presenting up-to-date knowledge and experience from institutions operating in another financial services sector.

The content of the training includes in particular the subject matter and basic concepts of the AML Act, due diligence of the liable person in relation to the client, the procedure for detecting UT and other obligations of liable persons, other provisions of the AML Act and links to other legislation, internal regulations of the liable person focused on the area of AML, penalties, or examples of possible abuse of the system. With the exception of a few institutions, AML training materials include a warning about the criminal consequences of violating AML legal standards. The information sources used to compile the content of the training are not defined in advance but are always based on own activities and at the same time take into account information originating from the public (NBS, Ministry of Interior of the Slovak Republic, PPF of the Slovak Republic, Moneyval, etc.), private sector (other securities dealers, banks, etc.), as well as foreign institutions in the field of AML.

Some companies also report participation in external foreign training courses, participation in conferences (BACEE, Slovak Compliance Circle and Czech Compliance Association). Various examples, statistics and studies from practice, etc. are used to better illustrate particular issues. All employees have access to internal guidelines, laws and other AML-related materials, both electronically and in hard copy.

The overall level of employees' knowledge of AML obligations (in particular the obligation to report UT, the ability to assess situations where there is an increased risk of AML, to understand the legal consequences in the event of a breach of obligations under the AML Act) was most often ***rated by institutions with*** a score of 1-2.5 (on a numerical scale of 1 - 5, best - 1, worst - 5). On the one hand, the above-mentioned range of numerical assessment reflects the staff's knowledge of the obligations arising from the AML Act, while on the other

hand it takes into account certain shortcomings, in particular in the area of client categorisation, identification of BO, monitoring of PEPs and sanctioned persons, or assessment of trades, and reporting of UTs.

D. Effectiveness of monitoring and reporting of UT in the capital market sector

The definition of UT under Slovak law is based on a demonstrative enumeration of the general forms of UT (Section 4(2) of the AML Act). Considering the wide range of liable persons, the legislator could not define by the AML Act all possible UTs that occur in the performance of individual activities covered by the Act, therefore, it obliged liable persons to develop and update the programme of own activities and to determine their own forms of UTs according to the subject of their business activities. This also applies to the capital market sector. The forms of UT according to the activities and types of trades carried out are part of the liable person's own activity programme pursuant to Section 20(2)(a) of the AML Act.

General forms of UT in the capital market sector can be considered, for example, if the client:

a) refuses to provide identifying information or data necessary to carry out the due diligence or refuses to declare on whose behalf he or she is acting,
b) who, by reason of his or her employment, position or other characteristic, may be presumed not to be, or to be incapable of being, the owner of the available funds,
c) where the amount of funds at the client's disposal is manifestly disproportionate to the nature or extent of the client's business or the client's declared assets,
d) where there is a reasonable expectation that the client or BO is a person subject to international sanctions or a person who may be related to a person subject to international sanctions, or the item or service is an item or service subject to international sanctions.

Other basic features and specific ways of recognising UT in capital market sector conditions may be if:

a) the client asks for the funds to be sent back (refunded) immediately after the conclusion of the contract,
b) the client asks for the funds to be sent back (refunded) immediately after the conclusion of the contract and at the same time asks for the funds to be sent to a bank account other than the one from which the money was transferred to the institution,
c) the client frequently changes the authorised bank account specified in the client documentation,
d) the client requests that funds from the sale of securities or from periodic collections of dividends/coupons on securities always be sent to a bank account other than an authorised bank account,
e) in the light of the information on the client's financial situation or the client's investment objectives as ascertained from the investment questionnaire, the transaction appears to be economically disadvantageous for the client,

f) the client's instruction to procure the sale of securities is given by an authorised person and that authorised person is also the purchaser of the securities,
g) the client is interested in purchasing securities from risky countries,
h) the client sends funds for the purchase of financial instruments from foreign accounts outside European Union member states,
i) the client deposits significant sums of money in cash for the purpose of procuring the purchase of securities or for the purpose of pursuing an investment strategy,
j) the client is a foreign national residing outside the Member States of the European Union,
k) an investor or client attempts to coerce an employee to breach his or her duty,
l) the investor or client provides false, confusing or contradictory information/documentation,
m) client's activities in "corruption-sensitive" sensitive areas, (e.g. public procurement),
n) is, for unknown reasons, nervous in face-to-face contact, accompanied and guided by a third person.

Similarly, a client's attempt to have minimal contact with the institution, a significant change in the number or volume of transactions or a significant change in the client's account balance, a transaction that is opaque in terms of its economic objective, or a transaction that appears illogical in design and may signal wrongdoing are all possible indicators of unusualness, the client provides false or misleading information, or refuses to provide routine information and supporting documentation for a business transaction without good reason, or provides information that can only be verified with difficulty by an employee of the institution or that is unreliable, etc.

Institutions are obliged to assess under the provisions of Section 14(1) of the AML Act whether the business being prepared or conducted is unusual. Institutions must therefore have the assessment of the unusualness of transactions regulated in own activity programme so that it is absolutely clear which persons assess the unusualness of upcoming or executed trades within their own structure, the time at which these persons carry out the assessment in question and the manner in which the assessment is carried out (in particular, by comparison with a review of the forms of UTs, etc.). Assessments should also be made on the basis of other information that staff have identified from available information e.g. risk profile, open sources with regard to the risk of ML/FT. The assessment of UTs is carried out by institutions from two perspectives:

d) the riskiness of the client - according to the "know your client" principle (KYC)
e) the nature, content and conduct of the trade.

Each UT must be evaluated by a competent staff member of the institution (applying the KYC principle). The detection of unusualness is done by continuous monitoring of individual trades according to the built-in criteria/scenarios. As a rule, institutions do not have a predefined exhaustive list of criteria for the assessment of clients/transactions, but take into account all the facts identified, both individually and in relation to each other. Thus, in the first instance, the

data provided by clients is assumed to be consistent, and if it is not, this either indicates a need to correct mistakenly stated inaccuracies and/or is an indicator of the presence of a higher risk.

Monitoring is usually carried out through an AML monitoring system (manual/automated - depending on the size of the institution) in order to identify unusual events or non-standard behaviour of clients and for each area the monitoring usually takes the following forms:

- continuous daily monitoring of operations - manual AML monitoring system - physically carried out by the responsible employee
- regular monitoring of operations - electronic AML monitoring system (based on predefined criteria) - triggered by the responsible employee
- search of lists (persons subject to international sanctions, countries at risk) - automated AML system - starts automatically.

The most common types of situations/scenarios pursued by institutions are e.g. account opening and closing in a short period of time, purchase and redemption of units in cash, operations carried out with high-risk clients, issuance or redemption of units with an extremely high value, multiple issuances or redemptions of units with a total absolute value that is extremely high, multiple smaller issuances of units apparently replacing a single issuance of units, etc.).

Initial monitoring is carried out by staff coming into direct contact with the client (e.g. staff in charge of concluding contracts for the issue of units, when concluding commission contracts), who should detect atypical transactions. As a rule, the responsible employee manually evaluates the transaction and, in case of suspicion, completes an internal "UT Report", which is sent to the Compliance Department by e-mail, fax or post without undue delay. The department concerned, after assessing the unusualness through the designated person, shall send the UT report to the FIU SR without undue delay.

Companies have UTs defined according to the AML Law, they take into account the specifics of their activities in their AML Program.

In the reporting period 2016-2019, companies captured and reported a total of 88 UTs to the FIU SR.

E. Client base profile - risk categorization of clients from AML perspective, client categorization, risk assessment and identification

Reported institutions use a risk-based approach to assess and manage risks under Section 20(a) of the AML Act, which is aimed at preventing the institution from being misused for ML/FT. In this context, the ***ML/FT risk level is generally distinguished in three levels: low, standard, high. The classification of a client in terms of risk into one of the above levels depends on the individual risk measures in the main risk categories, which are country risk, client risk and product risk.***

Companies state that they always carry out AML risk assessment prior to the establishment of a business relationship/prior to the execution of a specific trade and during the duration of the business relationship by means of monitoring software tools that process records in an electronic information system, or manually. They usually classify their clients into 3-4 risk categories, some companies use up to 5 risk categories (negligible, moderate, medium, high, unacceptable risk). Then, according to the risk category, they carry out the appropriate type of due diligence in relation to the client (basic, simplified, or enhanced due diligence). During the course of the business relationship, they regularly reassess the risk category of their clients as set out in their internal regulations and, on the basis of the reassessment of risk and monitoring of the client, they proceed to increase the risk category of the client.

Institutions assume that the classification of the client in each category is very important, but only a comprehensive ML/FT risk assessment will allow the appropriate type of diligence to be applied to a particular client. As a general principle, the more publicly available information about a client is available, the sooner the client can be classified into lower risk tiers. On the other hand, a non-transparent client for whom there is no credible information available will generally be classified at a higher ML/FT risk level, but this does not mean that the client will automatically be rejected or denied certain products or services. Classification of a client as higher risk means that the institution will take a heightened level of diligence in establishing a business relationship with the client, including a subsequent level of ongoing monitoring of the business relationship.

Country risk

The assessment of country risk depends for natural entities on the country of residence (resident, resident alien, non-resident alien), for legal entities on the basis of the country of domicile of the company. Countries with lower ML/FT risk are generally developed countries with transparent legal systems, low levels of corruption and stable independent financial markets, while countries with higher ML/FT risk are generally countries with high corruption indices, unstable economic and political conditions, inefficient and non-transparent legal systems, and benevolent business registration requirements. Finally, there are countries with standard ML/FT risk that cannot be explicitly classified into the above two groups.

Client risk

In assessing a client's risk, the institution shall base its assessment on the type of client and, in the case of a business entity, on the area in which the client operates and the ownership structure of the client. Lower-risk clients are generally public authorities either within the Slovak Republic or the EU, credit and financial institutions established in the EU or in a third equivalent country (with a similar ML/FT regime), a legal entity whose securities are traded on a regulated market of a Member State or an equivalent country, or multinational companies whose securities are traded on trusted stock exchanges. Information on the ownership structure as well as on the economic performance of these companies is generally publicly available.

In particular, a client can be considered as a **higher risk client** in terms of ML/FT if the client is:

- a person of whom the responsible person has knowledge that he or she is or has been suspected of criminal activities, in particular of a pecuniary or economic nature (e.g. theft, embezzlement, fraud, unjust enrichment, usury, tax evasion, etc.),
- a person employed or conducting business in an area with a higher risk of ML/FT (e.g. money changers, betting shops, gambling shops, etc.),
- a person permanently resident outside a Member State of the European Union,
- a person who is not a citizen of a member state of the European Union,
- an alien, in particular a natural or legal person, whose country of origin (citizenship, residence, domicile) does not sufficiently apply measures against the legalisation of proceeds,
- a person at higher risk of corruption (decision-maker, public official),
- a person who presents to the responsible person documents suspected of being forged, altered or lost,
- home-less person,
- shell company,
- a legal entity with an opaque ownership structure,
- a company that frequently changes its name and registered office,
- legal entity - a pool of assets (e.g. foundation, non-profit organisation, non-investment fund),
- PEP,
- a person on the list of sanctioned persons.

Such clients therefore require enhanced due diligence. An unacceptable client is, for example, a client who refuses to identify himself/herself or to submit to a check, with which the institution refuses to enter into a business relationship or to execute a specific trade or terminates the business relationship.

Some institutions, e.g. asset management companies, use a fully automated process aimed at calculating the overall risk exposure, implemented in the institution's respective application. However, the quality of this process is directly dependent on the quality of the data filled in when the client enters and/or edits data in this system. Once the overall risk rating has been determined, the relevant application will automatically alert you to the possible need to obtain additional information in order to adequately meet the legal requirements to exercise due diligence (e.g. in cases of political exposure (PEP) or high country, client or product risk, a risk rating of 3 equals the risk rating).

To identify and verify the identification of clients, institutions use publicly available sources such as the commercial and trade register, internet browsers, the company's GIN2ACT portal for the purpose of verifying persons in terms of PEP, embargos and sanctions http://ec.europa.eu/taxation_customs/taxation/gen_info/good_governance_matters/lists_of_countries/index_en-htm.

Institutions ascertain whether a client is a PEP by means of a declaration in the client's application and contractual documents (e.g. application for unitholder registration and issuance of units, portfolio management agreement) and subsequently verify the information provided by the client in publicly available sources.

Institutions use publicly available sources (e.g. commercial register, register of public sector partners, register of accounts, FinStat, register of final beneficiaries, etc.) to identify and BO, regardless of their risk category, and most institutions also require the submission of a declaration of honour.

***F*.** Products, business relations

The ML/FT risk assessment of products shall take into account the opportunities presented by each product or product line as well as its exploitability for ML/FT purposes. Products with standard ML/FT risk are generally products where payments reflect a specific business case about which the institution has information, the economic substance of which can be easily verified. A product with a higher ML/FT risk is a product where the level of client knowledge is limited or it is a product/service related to a cash transaction.

A securities dealer provides services to a predominantly retail segment of its client base. When establishing a business relationship, the client's answers in the investment questionnaire and the KYC questionnaire are considered, the required investment service, ancillary service or financial instrument, as well as the planned amount of investment are assessed. Subsequently, the compliance of the client's bank account with the authorised bank account specified in the contractual documentation and any deviations are assessed. The standard risk category includes a client who conducts business on his/her own account, with his/her own funds, and is also the BO, while the client does not conduct risky business activity or his/her profession is not classified in the special category (e.g. the client is not active in municipal or national politics, is not a public official, does not conduct a profession in which funds from the European Union are redistributed, etc.).

Management companies state as their main activity the creation and management of mutual funds - standard or alternative investment funds and the management of their clients' portfolios. Investments in mutual funds managed by asset management companies are made from accounts held in other banks (mainly in Slovak banks), from accounts held with the custodian, or are cash payments made through the trading outlets of the parent banks. All of these entities are obligated persons subject to the requirements of the Act. In terms of the riskiness of the product, the institutions report that the unit-linked product, subject to compliance with all legal conditions, presents a medium risk.

The institutions state that they see the greatest risk of laundering the proceeds of crime in investments through front-runners, seemingly unscrupulous persons and companies with foreign participation. In practice, a situation may arise where, in verifying information about a client and the origin of funds, the institution relies heavily on the veracity of the client's statement, while publicly available sources do not indicate any doubt as to the veracity of the

client's statement. In such a case, there is a high risk that the client will sophistically mislead the institution and thus the criminal proceeds used will be legalised in the financial system.

Institutions consider the creation of a single electronic system/database for all liable persons to be the most effective measure to prevent ML offences, which would enable a comprehensive verification of the client when concluding a business relationship or when carrying out specific transactions (e.g. to verify the authenticity of the identification document, to find out whether the client is a PEP, whether he/she is not on the list of sanctioned persons or persons prosecuted in connection with the laundering of the proceeds of crime and the FT, and so on).

Given the identified low risk of money laundering and terrorist financing, institutions may carry out simplified due diligence in relation to the client, subject to the conditions laid down for ***long-term investment savings.*** The long-term investment savings product is of general interest in the form of capital market development, it is subject to the supervision of the NBS, returns are realised only in the long term (15 years) with a maximum annual limit (EUR 3,000), as a result of which the conditions for its inclusion in the simplified diligence regime under Section 11 of the Act are fulfilled, as there is a low risk of ML/FT. However, the use of the simplified customer due diligence does not exempt the liable person from monitoring trades and business relationships sufficiently so that UTs can be detected and reported to the financial intelligence unit.

G. Emerging ML/FT risks

The NRA 2 questionnaire also included questions on identifying the risks associated with TF (identifying individuals who may be involved in TF, who maintain relationships with individuals based in war zones such as Syria Libya, Iraq, Ukraine Donbas, and who have contacts with foreign terrorists). All companies indicated that they had no identified clients in this area.

Other areas covered were the area of cum-ex schemes, clients with virtual assets and their coverage in internal regulations. With the exception of one firm, all firms stated that they did not have the areas covered in their internal regulations and one firm stated that their distributor had seen a minimal number of clients and their activity in the virtual asset area.

The questionnaire also focused on whether companies use modern methods and approaches when concluding a business relationship, i.e. whether companies apply the financial innovation FinTech, remote client identification. In the period under review, i.e. 2016-2019, only one company stated that it uses FinTech innovations in its operations and applies them in the business relationship with the client, e.g. facial and voice biometrics.

H. Feedback on the implementation of the conclusions of Round 1 of the NRA

The last question of the questionnaire survey aimed to find out what actions have been taken by the institutions after the 1st round of the NRA. Institutions reported that they have updated the company's own programme of work in light of the change in legislation, reviewed

risk factors in more detail, focused on improving the organisation and content of AML training (this includes the introduction of an e-learning application and expanding the range of training formats), placed increased emphasis on quality in the provision of information in UT reporting, and made sophisticated use of the IT system for the effective detection of UTs.

Institutions further indicated that they placed a high emphasis on screening the riskiest attributes within their client portfolios. In particular, the increased focus on risk attributes identified in the NRA have been reflected in a more detailed approach within the KYC client review process. New modern IT application facilities have been introduced in the areas of monitoring, controls, UT reporting, KYC onboarding and KYC review processes to simplify and streamline AML management. In only 1 case did the company state that due to the structure of the company's clients and the low percentage of occurrence of risk factors among its clients, the company did not apply the additional AML measures from the conclusions of the Round 1 NRA.

4.1 Summary of the NRA 2 questionnaire survey

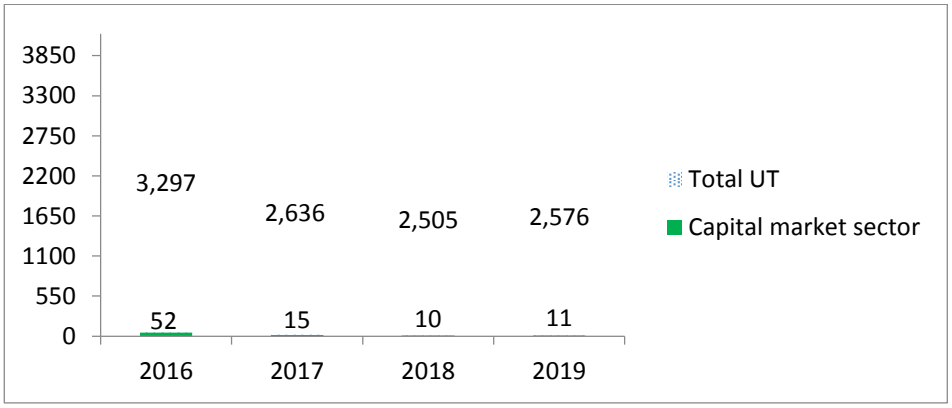
This part of the risk assessment was mainly based on the responses of the institutions contacted, which can be summarised as follows:

- ***the sector has a good theoretical knowledge of AML/CFT prevention;*** (The numerical rating (1-2,5) on the one hand reflects the knowledge of the AML/CFT staff, but at the same time, on the other hand, takes into account certain shortcomings, in particular in the areas of client categorisation, detection of BOs, monitoring of PEPs and sanctioned persons, and assessment of trades, respectively),
- institutions have developed risk management policies that identify, assess and take measures to mitigate risks, based on a risk-based approach pursuant to Section 20a of the AML Act; institutions most commonly distinguish ML/FT risk measures in three levels (low, standard, high); the classification of a client's risk into these levels depends on the individual risk measures in the main risk categories, which are country risk, client risk and product risk,
- institutions have a regulated overview of the forms of UT according to the subject of the liable person's activities,
- institutions have AML ***monitoring systems*** (manual/automated depending on the size of the institution) to identify UTs,
- one company indicated in a questionnaire survey that they had started using biometric identity verification to verify client identity,
- higher client/product risk is subject to increased scrutiny (frequency of monitoring, extent),
- ***the designated person has precisely defined rights and duties*** in the organisational structure of the company, as well as organisational and material security for the independent performance of his/her function,
- Institutions have other internal regulations in addition to their own agenda, such as a Code of Ethics or Rules for Reporting Possible Violations of Internal and External Rules, an Insider Policy, a Conflict-of-Interest Policy, or a Compliance Manual, in which the conditions of integrity of employees are regulated,

- - no suspected intentional criminal offences of a pecuniary nature committed by staff members were recorded by the institutions contacted during the period under review. However, two companies recorded 2 breaches in the area of conflict of interest during the period under review.
- the sector has not identified, on the basis of the questionnaire, increased risks associated with terrorist financing, identifying persons who may be related to TF, who maintain a relationship with persons based in war zones,
- the sector has not seen an increase in risk associated with the provision of virtual assets.

5. THE EFFECTIVENESS OF MONITORING AND REPORTING OF UTs

In this assessment period, the FIU SR records the largest number (approximately 95%) of the total number of reported UTs from banks, where the largest volume of funds and the related number of trading operations are concentrated. The FIU SR experience to date, as well as the experience of the banks, demonstrates that the greatest efforts to misuse liable persons for possible ML/FT are again directed by potential perpetrators towards products and services provided by banks. The dynamics of the evolution of the UT reports received between 2016 and 2019 were as follows:



Out of the total number of reports in the period under review (2016-2019), the FIU SR received a total of ***88 UT reports*** in the capital market sector, namely 54 reports from asset management companies, 8 reports from central depositories and 16 reports from securities dealers. Compared to the previous assessment period (2010-2015), when the FIU SR received a total of 221 UTs in the securities sector, there has been a significant decrease in UTs. This was partly influenced by the fact that NRA 1 was carried out over a period of up to six years and, in addition, pension management companies were included in the securities sector.

Out of the total number of reports received on UTs in the capital market sector, 62 were entered into the FIU SR comprehensive information system (database) for possible further use. After a thorough analysis of the received reports on UTs, processing and subsequent evaluation, taking into account the identified facts that were relevant for specific subjects, the FIU SR provided the National Criminal Agency with 8 pieces of information, the Financial Administration with 11 pieces of information, foreign FIUs with 5 pieces of information, regional and district directorates of the PF with 2 pieces of information.

The reported operations generally involved: cash deposits of an unusually large amount (approx. over EUR 200 000), usually at a branch of the parent bank or at a post office for the purpose of purchasing units; deposits and subsequent withdrawals of large sums within a short period of time and subsequent re-deposits; gratuitous transfer of shares between two legal entities; issuance of shares by an issuer that was a shell ready-made company or a company domiciled in an offshore country; securities were transferred in concert without financial settlement by DWP - delivery without payment to an entity domiciled in a sanctioned country, etc.

Often situations have been reported where a client has applied for the issuance of units in a higher amount (EUR 100,000), which has been transferred from an account held with a commercial bank to a mutual fund account. ***However, it was not clear from these reports for what reason the transaction was assessed as unusual, nor whether and how much due diligence was carried out by the liable person in relation to the*** client (ascertaining the origin of the funds, the BO, etc.).

Deficiencies resulting from UT reporting:

- due diligence is not consistently exercised in relation to the client,
- when assessing trades, there is no emphasis on identifying the origin of funds at the entry into the financial system,
- the unusualness of the reporting is oriented towards the exit of funds from the financial system (redemptions, termination of a business relationship)
- a common reason for determining unusualness is the purchase of fund units in a certain amount (e.g. above EUR 150,000),
- high-risk ML clients are allowed to reinvest in units; the origin of the funds is not ascertained,
- despite the risk profile of the client, the institution continues the business relationship and reports the client after each trade is executed,
- UT reporting lacks information on basic due diligence provided,
- failure to assess specific client trades during the term of the mandate agreement with the issuer, reporting substandard handling of funds after termination of the mandate agreement,
- the overall poor quality of UT reporting as well as trade assessment records.

In general, the analysis of the UT reports showed that institutions did not investigate the origin of funds entering the financial system, allowed the entry of "possible" illicit funds and subsequently reported it, or only reported the exit of funds from the system.

6. SURVEILLANCE RESULTS (overview of weaknesses and strengths of supervision)

The compliance function plays an important role in preventing and combating ML/FT. Integrated supervision of institutions in the capital market sector is carried out by both the NBS and the FIU SR. The basis for the implementation of the control activities was mainly the annual control plan, in the elaboration of which the knowledge from specific developments in the field of protection against ML/FT and the knowledge gained from previous surveillance activities were used. The results of cooperation with other supervisory authorities were also used in order

to exchange information and transfer specific knowledge useful in the performance of control (supervision), to make it more efficient, as well as to avoid duplication in the individual supervision of liable persons.

NBS carries out:

1. comprehensive supervision - supervision of the overall activity of the company, detailed, analytical;
2. thematic supervision - supervision of selected activities of the company (e.g. investment services, AML);
3. tracking surveillance - checking the measures taken to address deficiencies identified during comprehensive or thematic surveillance.

The subject of the NBS supervisions in the securities sector was compliance with the Act on Collective Investment, the Act on Securities and Investment Services and, in the framework of the comprehensive supervisions carried out, also compliance with the AML Act and other generally binding legal regulations applicable to the supervised entity or to its activities..

Within the framework of risk-based supervision, the NBS has developed the Instruction of the Head of the Securities Market and Pension Savings Supervision Department for the protection against ML/FT of a securities dealer, which entered into force on 1 June 2018 and which regulates the characteristics of the risk-based approach to the conduct of supervision against ML/FT and the steps in the conduct of risk-based supervision as required by Article 48 par. 10 of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of ML/FT, amending and repealing Regulation (EU) No. 648/2012 of the European Parliament and of the Council Directive (EU) of the European Parliament and of the Council 2005/60/EC and Commission Directive 2006/70/EC.

A total of 9 thematic supervisions were carried out in the area of collective investment during the assessment period 2016-2019. No findings and deficiencies were identified in the AML area during the reporting period.

In the assessment period 2016-2019, a total of 19 supervisions were carried out in the area of securities markets, including 5 comprehensive, 14 thematic and 1 follow-up supervision. In the AML area, the following deficiencies and findings were identified in the securities dealer sector during the reporting period: ***failure to appoint a designated person and a deputy designated person responsible for ML, failure to adhere to the staff training schedule, late reporting of UTs, insufficiently drafted and updated internal rules.***

The FIU exercises comprehensive supervision of compliance with AML obligations. The risk-oriented approach to conducting the inspection is regulated in Article 2.1 of the Order of the Director of the FIU SR National Criminal Agency No. 126/2018 and in the Methodological Guideline on the procedure of inspection of compliance with the obligations of liable persons arising from the AML Law by the police officers of the Inspection of Liable Persons Department of the FIU SR National Criminal Agency No. 34/2018.

In accordance with the AML Act and the Examination Plan, a total of three examinations were conducted by the FIU SR at institutions in the securities sector between 2016 and 2019, namely at securities dealers.

The inspection of the FIU SR focused on the fulfilment and compliance with the obligations of the liable person, in particular from the AML Act, namely Section 20 - development and updating of the program of own activities aimed at AML/CFT, Section 10 to 12 - implementation of due diligence of the liable person in relation to the client, Section 14 to 18 - the procedure for the detection, assessment, refusal of the trade, delay and reporting of UT, compliance with the obligation of confidentiality, and other violations of the provisions of the law found during the audit of the liable person.

The most frequent deficiencies identified during the inspection were failure to elaborate mandatory elements in the programme of own activities, failure to identify the origin of funds or the BO and failure to take appropriate measures to identify the ownership and management structure of the client and the subsequent refusal to enter into a business relationship, failure to report the UT without undue delay. Other deficiencies identified related to improper manual treatment of client risk from an AML/CFT perspective, failure to assess individual trades, failure to maintain records of assessments, failure to exercise due diligence, etc. Some transactions were not assessed in accordance with the KYC principle or the results of the assessment were not justified to show what considerations and reasons led to the conclusion that a particular transaction was usual or unusual.

In one case, a securities dealer was found to have performed payment services that were unrelated to the management of the client's securities and for which he was not authorised under the Securities Act (funds for the alleged acquisition of securities were credited from an account other than the one specified by the client for no apparent reason and were subsequently immediately transferred offshore to a third party's account).

It was also found from the audit activity of the FIU SR that in the practical activity of the Central Securities Depository there were situations when issuers that are not a regulated entity or an entity whose shares are not publicly traded applied for the registration of the issuance of debt securities in a relatively high volume ranging from EUR 5 million to EUR 30 million. The issuers were usually foreign entities based in offshore countries (and thus could be considered geographically risky in terms of ML/FT protection) or newly established ready-made companies that had only virtual seats in Slovakia (shell companies). The legal form of the companies was usually a limited liability company, with a minimum share capital, the issuers did not actually carry out the declared business activity, the BOs in the companies were natural persons domiciled outside the territory of the Slovak Republic, usually in the countries of the former Soviet Union or in offshore countries.

The companies' assets and their economic situation, according to available sources, were disproportionate to the amount of liabilities arising from the issue of debt securities without further backing (e.g. the existence of a parent company which set up a subsidiary for investment purposes, etc.) or other security for the liabilities. At the same time, the legislation made it relatively easy to wind up/liquidate without holding specific persons liable for the company's failure to meet its obligations.

These were private bond issues where the NBS does not supervise the issuance of securities. The increased AML risk consisted in the fact that it was a private placement of securities, where **neither a rating nor the preparation and submission of a prospectus subject to the approval** of the NBS was required. According to the findings of the FIU SE, only in the case of 4 issuers, the amount of individual issues of bonds issued amounted to a **large volume of funds with a total value of approximately EUR 96 million**.

Unusual from the point of view of the economic purpose of the issue was that the subscription documents agreed on a settlement date with a condition precedent of up to 3 months from the acquisition of the bond. After the property settlement of the primary subscription, the initial purchaser became the owner of the Bonds at the time of non-payment for the purchase of the Bonds, and prior to the expiry of the deadline for payment of the financial obligation under the primary subscription agreed in the underwriting document, the initial purchaser sold the Bonds to another entity domiciled in the Russian Federation or to an entity whose directors and shareholders were persons with citizenship of the Russian Federation. The adjustment of the 3-month postponement of the payment of the issue price of the bonds acquired from the issuer (upon their issuance) was extremely unusual and such a procedure did not make any obvious economic sense, as the common practice is that the payment precedes the issuance of the bonds and their delivery/assignment to the first owners, or the issuance of the bonds is carried out by the method of "delivery versus payment" (delivery of the bond versus the payment - the financial settlement/payment).

Funds received from the Russian Federation were transferred immediately after crediting by clients to other foreign accounts, between several countries (Cyprus, Singapore, Taiwan, Liechtenstein, Estonia, Great Britain, Latvia, Switzerland, Thailand, Panama, San Marino, etc.), the transactions were directed to areas where it could not be assumed that the clients had business interests, suggesting that ***these activities were carried out in order to obscure the true origin of the funds and to obscure their flows.***

From the foregoing, there is a reasonable presumption that the securities dealer, through a scheme to "prefinance the operational needs" of a select group of clients and the subsequent trading of bonds among a narrow range of investors on a free delivery basis (without financial settlement), circumvented the law and aided and abetted the laundering of the proceeds of crime.

On the basis of the inspections carried out in the period under review, the IU SR initiated administrative proceedings under administrative sanctions in two cases, in which decisions to impose fines totalling EUR 47,000 were issued. Sanctions have so far been imposed in lower bands, taking into account the preventive effect and the educational nature of the sanction, which, however, may not have been sufficiently effective and deterrent in some cases.

6.1 Availability and enforceability of administrative sanctions

The regulation of administrative sanctions is contained in Section 32 - Section 34 of the AML Act, as well as in specific regulations in the field of capital market. The FIU SR may impose a fine of up to EUR 1,000000 on the liable person for non-compliance or violation of the obligations arising from the AML Act, or up to EUR 5,000,000 for banks and financial

institutions, pursuant to Section 33 of the AML Act. The financial intelligence unit may also impose an obligation to refrain from unlawful conduct or to remedy the deficiencies detected. Pursuant to the provisions of Section 33a of the AML Act, in addition to the fine for administrative offences referred to in Section 33(1) and (2), the Financial Intelligence Unit may also impose on a legal person or entrepreneur the sanction of disclosing the final decision on the imposition of the sanction.

Pursuant to the provisions of Section 34 of the AML Act, if the liable person fails or repeatedly fails to fulfil or violates the obligations laid down in the AML Act for more than 12 consecutive months or repeatedly, the FIU SR shall file a petition for revocation of the authorization for entrepreneurial or other self-employed activity with the authority authorized to decide under a special regulation.

If the NBS detects breaches of obligations arising from special laws or generally binding legal regulations, including the AML Act, related to the activities of supervised entities, or deficiencies in their activities, or non-compliance with measures imposed by a decision of the NBS, the NBS may impose various types of sanctions on all supervised entities according to the provisions of the legislation, e.g. measures to eliminate and remedy identified deficiencies, a fine, may order the replacement of senior management or the employee responsible for the performance of the compliance function, suspend for a specified period of time and to a specified extent the handling of the Fund's assets and the issuance of the Fund's securities, prohibit or suspend the distribution of securities, order the cessation of an unauthorised activity, restrict the performance of an authorised activity, revoke the authorisation granted, or order the establishment of an internal audit function or a risk management function.

It is also possible for the NBS to impose on a member of the board of directors, a member of the supervisory board of a management company, a proxy of a management company or the head of a branch of a foreign management company or a foreign collective investment undertaking for violation of the obligations arising from the AML Act, from other generally binding legal regulations, from the articles of association, etc. a fine of up to twelve times the monthly average of its total revenues received from the management company, from the foreign collective investment undertaking, from the foreign management company, according to the gravity and nature of the infringement. A fine of up to 50% of the aforementioned amount may be imposed on the senior management, the employee responsible for the performance of the internal audit or risk management compliance function or the deputy head of the branch, depending on the gravity and nature of the breach. Such a person who has ceased to be a trustworthy person by the final imposition of a penalty shall be immediately removed from office by the institution.

The NBS may impose a penalty on a member of the statutory body or a member of the supervisory board of a securities dealer or a central depository, the head of a branch of a foreign securities dealer and his deputy, a forced administrator of a securities dealer, a proxy, an employee responsible for the performance of internal control or a senior employee of a securities dealer or a central depository for breach of duties, arising from this Act or from other generally binding legal regulations, including the AML Act, or for violation of conditions or obligations imposed by a decision issued by the NBS, shall be fined or imposed a temporary

ban and, in the case of a repeated serious violation, a permanent ban on exercising the functions of a member of the management body.

7. Vulnerability assessment and risk analysis in individual institutions

The choice of the capital market sector to be analysed in detail was conditioned by a number of factors such as:

- segment size,
- the degree to which it is exposed to ML/FT threats,
- the estimated volume of client assets under management,
- number of reported UTs,
- relevance to threat detection,
- the severity and diversity of these threats, etc.

In terms of assessing the real risk of vulnerability in each area (institution) to ML/FT the following scores have been identified accordingly:

A. In the area of collective investment (asset management companies), **the risk score was set at 0.58 - medium** based on the input data, which means that the risk of money laundering in this area is present, **but to a lesser extent than in the case of banks.**

However, the aforementioned area is sufficiently secured due to the fact that collective investment products (investments in mutual funds managed by a management company) are made in a non-cash manner through banking institutions (mainly Slovak banks), or in cash through the trading outlets of financial institutions, while these entities are liable persons, who are subject to the requirements of the AML Act and strict regulation. However, the extent of investments received in cash in mutual funds managed by the management company is negligible.

The risks of doing business in this area are similar to those in other sectors, especially banking. Risk may be posed by transactions executed on behalf of another person, opaque follow-on transactions, transfers of securities between entities domiciled in different countries, receipt of funds from clients in non-standard countries and regions, such as off-shore, in the case of clients with unclear ownership structures, risky, sanctioned countries and situations where there is a presumption that such clients have large amounts of funds at their disposal, the origin of which may be problematic from an AML point of view.

Mutual fund units can therefore be considered as medium risk products in most cases (taking into account the nature of the product, possible transactions, potential clients, distribution channels and the existence of negative evidence regarding ML/FT). However, the measures need to be mainly based on risk-based due diligence on the client and monitoring of UTs through appropriately calibrated AML scenarios.

In the period 2016-2019, the volume of assets in collective investment funds grew by EUR 2.7 billion, resulting in EUR 9.6 billion of client assets collected in both UCITS and AIF funds as of 31 December 2019.

With the increase in assets, the number of clients and the number of transactions has also increased, which requires greater emphasis on the process of client identification and the monitoring of UTs by asset management companies. According to the questionnaire survey, management companies cited the increased risk of investments made through shell companies with seemingly unimpeachable foreign participation, misleading portfolio construction and property acquisitions in connection with the transfer of ownership of criminal assets, and an increase in the number of clients as increased risks. Another risk appears to be the current introduction of new modern methods and approaches in the conclusion of a business relationship, remote client identification, as well as the emergence of new companies and their entry into the capital market, ***which influenced an increase in the score compared to the previous assessment in NRA 1 from 0.53 to 0.58 .***

The above clearly indicates that there is still a danger associated with the growing risk of ML and therefore it can be concluded that the vulnerability of this sector is at a medium level.

B. In the area of securities markets (securities dealers), the risk score has been stabilised at 0.41 - medium based on the input data, which means that the risk of ML in this area is present, but to a lesser extent than in the case of asset management companies. Securities dealers are predominantly small companies with a small number of clients, relationships with them are conducted on a personal basis and for this reason the institution's employees are familiar with the clients' circumstances as well as their financial and property situation, risk and investment profile.

Securities dealers generally operate on a cashless basis, i.e. any financial transactions and transfers are carried out through the client's and the securities dealer's bank accounts. For this reason, in addition to monitoring by the securities dealer, the client is also subject to monitoring by the bank or financial institution which, at the client's order, makes payments to the client's account for the benefit of the client in question.

However, the risk of introducing new modern methods and approaches in the conclusion of the business relationship, the identification of the client at a distance, as well as the emergence of new companies and their entry into the capital market must be taken into account.

As noted in Section 6, one securities dealer was found, in relation to private placements for which it had secured registration with the CSD, to have allowed a group of clients with a heightened risk profile to create patterns in securities trading that could be considered ML phases designed to obscure asset transactions and conceal the illicit origin of the proceeds of crime in order to disrupt the ability to trace the flow of money and to cover their tracks. This showed that the securities dealer, through a scheme to "refinance the operational needs" of a select group of clients and the subsequent trading of bonds among a narrow range of investors on a free delivery basis (without financial settlement), circumvented the law and facilitated the laundering of the proceeds of crime.

Therefore, there was an increase in the score from the previous assessment in NRA 1 from 0.37 to 0.41.

C. For the activities of stock exchanges and central depositories, based on the input data, the ***risk score was stabilised at 0.16 - low***, which means that the risk of ML in this area is present to a low degree, as the above institutions operate on a membership basis, which means that the members are banks, securities dealers, asset management companies and other financial institutions that operate on the basis of the NBS authorisation and are liable persons under the AML Act.

However, as the NRA 2 questionnaire showed, from the perspective of the Central Securities Depository, bond issuance, which is not restricted in any way and is also not supervised by the NBS (except for statutory exceptions), appears to be risky for the AML area**.** The restriction on the issuance of bonds applies only to natural entities. Any legal entity may issue bonds, to any extent, without restriction and without being supervised.

As a rule, even in the case of unusually high issue volumes, foreign issuers (even with links to offshore countries), from owners with opaque ownership structures, etc., the legal requirements for registration and issuance of the bond issue are always met. In no case may the CSD refuse to register an issue, for example, because of doubts about the issuer's creditworthiness or the purpose of the issue.

Therefore, there was an increase in the score from the previous assessment in NRA 1 from 0.02 to 0.16.

7.1 Transnational Risk Assessment by the European Commission

In terms of the Transnational Risk Assessment by the European Commission in relation to institutional investing - (securities, asset management and investments) this report states that there are a number of scenarios in which perpetrators may commit abuses against investors or the financial markets, for example through the integration of proceeds, owning shares to conceal beneficial ownership, through fraud or market abuse, brokerage accounts, investments to justify the proceeds of crime as profit, predicate investment fraud or investing proceeds using specialist financial services with a high rate of return on the proceeds.

Threat of FT

This FT threat could be significant if large amounts of legal funds are invested to finance terrorism, but when it comes to generating small amounts to commit terrorist attacks, the terrorist financing threat is not significant for this product/sector. **The threat level is considered to be minor (level 1).**

Threat of ML

The growing role of intermediaries in ML schemes may expose the sector to such threats, although knowledge and expertise are needed to implement them. Although it is possible to raise a large amount of funds through this process, it is not simple in terms of access and therefore criminal organizations do not prefer this kind of risky scenario. Nevertheless, several methods have been identified in recent years to move large amounts of illicit funds, prepared by very clever intermediaries:

- capital market clients in commodities who execute over-the-counter trades in futures and swaps through exchanges and use illicit means for settlement after expiration;
- the simultaneous purchase, transfer and sale of securities between the countries of two apparently unrelated but mutually controlled entities;
- capital market clients who trade bonds on behalf of organised criminals use illicit money to buy bonds and, after selling these bonds, deposit the funds in financial institutions.

In this context, the threat of ML in relation to institutional investment is considered **to be significant (level 3).**

Vulnerability to FT

Vulnerability to FT in the context of institutional investment is a less significant inherent risk. The various risk factors, products, clients, geographic location and delivery methods in this sector mean that this product/sector is not preferred for FT purposes. Perpetrators typically do not have the expertise to access this sector, while the small amounts of money used for terrorist attacks have made other sectors attractive for their purposes. **Vulnerability to FT is considered minor (level 1).**

Vulnerability to ML

In its assessment of ML vulnerabilities in relation to institutional investment, the EC made the following findings:

a) exposure to risk

The main factor mitigating the inherent risk associated with ML is the low level of cash-based transactions, despite the fact that the sector is exposed to high-risk clients, including PEPs, while the volume and level of cross-border transactions are high. For criminals to have access to this sector, they must deposit money through the banking system, and hiding illicit money through opaque structures requires a high degree of expertise. Banks are therefore the first barrier that mitigates the inherent risk of ML.

b) risk awareness

For transactions outside the banking sector, the awareness of risks in this sector is not high. This is because institutions typically rely on banks to exercise customer due diligence and customer monitoring when money enters bank accounts.

Supervisors consider the overall risk of the sector to be moderately significant; however, the risk profile at the institution level shows that a significant proportion of institutions are classified as a less significant risk. Nevertheless, most supervisors consider this sector to be a very significant cross-border risk. Another key risk to which the sector is exposed is the alignment of ML standards in home and host Member States where the Group's branches are located in different countries.

According to financial intelligence units, the number of suspicious transaction reports is relatively low compared to the volume of transactions involved, as the sector is more aware of the need to detect fraud, such as insider dealing or market abuse, and less aware of suspected ML. At the same time, the financial transactions involved are more complex and suspicious transactions are likely to be more difficult for liable entities to detect.

The sector also faces a significant conflict of interest between ML concerns and the need to attract clients, some of whom are at high risk of ML, such as PEPs, clients from high-risk non-EU countries and high-income clients. In this sense, the fact that the service is provided by an intermediary affects the level of vulnerability to ML, thereby increasing the vulnerability relative to the vulnerability in relation to credit institutions.

c) legal framework and inspections

Institutional investments through brokers are subject to AML/CFT requirements at EU level. However, the quality of the implementation of this legal framework is questionable. In the investment field, the client manager has an interest in managing the business relationship (for the sake of remuneration/fees) and this may lead to his/her being more restrained in the exercise of due diligence in relation to the client.

Supervisors believe that weak controls limit the effectiveness of suspicious transaction reporting and the effectiveness of ongoing monitoring policies and procedures, including transaction monitoring. On the contrary, most of the infringements found during inspections were considered to be minor. The most frequent finding was weak controls on PEPs.

Conclusion: Exposure to risk is high by nature due to the nature of the clients and the large sums involved in the transactions. However, the inherent risk is mitigated by the low level of cash-based transactions. When investment services are provided by "brokers", the vulnerability to ML is higher than when these services are provided by banks. Lack of resources to apply robust due diligence procedures in relation to the client and certain conflicts of interest in attracting clients with a high-risk ML profile may increase vulnerability. **In this context, the ML vulnerability of institutional investment provided by brokers is considered to be significant (level 3).**

8. Identified weaknesses in the capital market sector and proposals for action

The shortcomings identified relate in particular to:

- **non-standard trades in financial instruments,**
- prioritising trading policy over AML policy
- low number of inspections by the FIU SR,
- the level of supervisory fines imposed, which is not sufficiently dissuasive,
- **lower awareness of ML/FT risks among new entities.**

The risk assessment carried out showed that the FIU SR does not have sufficient resources (technical capacity, budget, funds) and trained staff in the Control of Liable Persons Department. Currently, it is not possible for FIU SR employees to acquire the necessary skills and up-to-date knowledge to control compliance with anti-ML/FT legislation, as they do not

attend the necessary professional seminars, trainings, conferences, etc. due to workload and lack of funds. Due to inadequate staffing of the FIU SR, the necessary number of inspections of liable persons in the securities sector were not carried out. Compared to the FIU SR, the NBS has a larger number of trained supervisory employees. Employees are provided with the technical means to perform their work as well as opportunities to participate in AML training.

PROPOSED MEASURES:

- emphasize strict compliance with legislation and conduct customer due diligence or enhanced customer due diligence when applying the know your customer ("KYC") principle,
- comprehensively assess trades and perform transaction monitoring,
- identify and manage the risks associated with the investment strategy of institutions, in particular in relation to non-standard trades in financial instruments,
- conduct regular training, coaching and seminars on AML compliance,
- increase the number of inspections by the FIU SR,
- impose stricter sanctions for violations of the AML Act by both the NBS and the FIU SR,
- resolve the issue of staffing, material and technical support for the FIU SR.

Since the Central Securities Depository may refuse to register a bond issue only if the legal requirements for such registration are not met, or if the registration is not completed or if the issuer fails to prove that they have been met or if the issuer fails to pay the relevant fees, and in any case cannot refuse registration of an issue on the grounds of doubts about the issuer's creditworthiness or the purpose of the issue, the SR should proceed to amend the relevant legislation to prevent the registration of private bond issues by shell companies or the possibility for the Central Securities Depository to refuse substandard bond registration.

The primary objective is therefore to raise awareness of AML/CFT, education, guidelines and recommendations for liable persons under the AML Act, as the quality of training, the theoretical preparedness of employees coming into contact with potential UT, the quality of technical support and the quality of the UT itself defines the quality of the institution in the securities sector in the area of prevention of ML/FT.

In all stages of the ML process, however, ***banks and the banking system play a key role***. Employees of banks, but also of other institutions that come into contact with clients, should be trained to identify UTs.

In the securities sector, it can be stated that ML/FT risks are lower than in banks, as long as client funds are received or sent to the institution exclusively by means of wire transfers and the standard measures on fund transfers are applied to them (Section 10, Section 12, Section 14 of the AML Act).

The risk increases when funds are transferred from countries where the origin or the client/BO cannot be identified. On the other hand, it should be noted that most financial instruments are in book-entry form and bearer, which significantly reduces the possibility of concealing ownership, which is significant from a ML perspective.

It is therefore essential both to eliminate illegal sources from entering the system and to prevent the system itself from being abused to commit crime. In this context, it should be stressed that banks and the banking sector, in particular, should strengthen the entire monitoring system in the area of ML, which has a consequent impact on the capital market area and is mainly related to the reputational risk of the entire financial sector.

Evaluation of the Action Plan – NRA 1

1. the FIU SR carried out inspections at a very small number of institutions in the securities sector.

On the basis of the evaluation of NRA 2, we can conclude that the FIU SR continues to provide insufficient material, technical and personnel support for the performance of inspections of liable persons. In accordance with the AML Law and the Examination Plan, a total of three examinations were conducted by the FIU SR at institutions in the securities sector between 2016 and 2019, namely at securities dealers.

Insufficient awareness of ML/FT risks and their management, or ineffective implementation of AML prevention measures/non-compliance with otherwise sufficient legislation

In the area of legislation, in the period 2016-2018 the NBS issued the Methodological Guideline of the Financial Market Supervision Unit of the National Bank of Slovakia of 13 May 2019 No. 6/2019 on protection against ML and protection against FT in the activities of a securities dealer, branch of a foreign securities dealer, asset management company, pension management company and supplementary retirement company, and FIU SR issued a number of methodological guidelines for the mandatory AML area, **which improved the awareness of ML/FT** risks in the sector.

The guidelines in question are regularly published on the NBS and FIU SR websites.

2. NRA 1- Employee training is mostly formal in order to fulfil the obligation under section 20(3) of the Act, often without practical result

Based on the analysis of the NRA2 questionnaire, it can be concluded that the liable persons have improved the quality of training for their employees in this area. In particular, they focused on the areas of: due diligence of the liable person in relation to the client, the procedure for the detection of UTs and other obligations of liable persons, the internal rules of the liable person focused on the AML area. The content of the training focused on examples of potential abuse of the system, with emphasis on the use of various examples and case studies, etc.

NRA1- deficiencies arising from UTs, inconsistently performed due diligence in relation to the client, assessment of trades, unusual and poor quality of UT reporting

The analysis of the UT reports in the reporting period 2016-2019 showed that the institutions did not ascertain the origin of the funds at the entry into the financial system, allowed this entry of "possible" illegal sources and subsequently reported it, or only reported

the exit of funds from the system, which means that **we have to conclude** that the above-mentioned **shortcomings still persist**.

LIST OF ABBREVIATIONS

AML/CFT	– Anti-Money Laundering / Countering the Financing of Terrorism
AML Act	– Act No. 297/2008 Coll. on protection against money laundering and terrorist financing and on the amendment to certain acts as amended
AMO	–Asset Management Office
Cybercrime	– computer-related crime
CDD	– customer due diligence
EEC	– European Economic Community
EU	– European Union
FATF	– Financial Action Task Force
FD SR	– Financial Directorate of the Slovak Republic
FA SR	– Financial Administration of the Slovak Republic
FIU SR	– Financial Intelligence Unit of the National Crime Agency of the Presidium of the Police Force - (Financial Intelligence Unit of the Presidium of the Police Force)
GPO SR	– General Prosecutor's Office of the Slovak Republic
GDP	– gross domestic product
RH PF	– Regional Headquarters of the Police Force
FACO	– Financial Administration Criminal Office
BO	– beneficial owner
KYC	– "Know Your Customer"
MEKO	– Interdepartmental Expert Coordination Body for Combating Crime
MF SR	– Ministry of Finance of the Slovak Republic
NES - LP	– National AML/CFT Expert Group
ML/FT	– Money Laundering and Terrorist Financing
MD SR	– Ministry of Defence of the Slovak Republic
MJ SR	– Ministry of Justice of the Slovak Republic
MI SR	– Ministry of Interior of the Slovak Republic
NBS	– National Bank of Slovakia
NRA	– National Money Laundering and Terrorist Financing Risk Assessment
UT	- unusual transaction
OECD	– Organisation for Economic Co-operation and Development
AF SR	– Armed Forces of the Slovak Republic
DH PF	– District Headquarters of the Police Force
PPF	– Presidium of the Police Force
SIS	– Slovak Information Service
SR	– Slovak Republic
SPO GPO SR	- Special Prosecution Office of the General Prosecutor's Office of the Slovak Republic
MI	– Military Intelligence
V4	– Visegrad Group of countries (Visegrad Four): Czech Republic, Poland, Hungary, Slovak Republic
WBG	– World Bank Group