



**MINISTRY OF INTERIOR OF THE SLOVAK REPUBLIC  
PRESIDIUM OF THE POLICE FORCE**

National Criminal Agency  
Financial Intelligence Unit

PPZ-NKA-FSJ-59-017/2019-PZ

Bratislava 17.04.2019



**Annual Report  
of the Financial Intelligence Unit  
for 2018**

Submitted by:  
pplk. Ing. Peter Čarnecký  
Deputy Director

Subject matter:  
Information about  
FIU's activities and  
results for 2018

Bratislava

## Content

<b>Introduction .....</b>	<b>3</b>
<b>1. Financial Intelligence Unit .....</b>	<b>3</b>
<b>2. Unusual business transactions .....</b>	<b>4</b>
2.1. Selected cases of UBT treatment .....	13
2.2. Forecasts of further development in ML and TFarea .....	17
<b>3. Control and legislative activities .....</b>	<b>18</b>
<b>4. International cooperation .....</b>	<b>20</b>
4.1. Forms of cooperation .....	20
4.2. Methods of international cooperation .....	20
4.3. FIU's involvement in international organizations .....	21
<b>5. Cross-border reporting .....</b>	<b>22</b>
<b>6. Evaluation of cooperation with partner entities .....</b>	<b>23</b>
<b>CONTACT DATA .....</b>	<b>25</b>

## Introduction

The Financial Intelligence Unit of the National Criminal Agency of the Presidium of the Police Force (hereinafter only the "FIU") hereby submits its annual report summarizing the activities of 2018.

The purpose of the report is to provide a comprehensive view of the present developments in fight against legalization of proceeds from criminal activities and terrorist financing in 2018 in the Slovak Republic (hereinafter only the "SR") including defining of forecasts of their further development and direction. The text and the graphic illustrations provide relevant statistic data in the area of assessment of unusual business transactions, control activities, international cooperation and analytical activities for the last year

As to those FIU activities which cannot be quantified, it is necessary to draw attention to finalization of the process of national assessment of money laundering and terrorist financing risk in the SR (hereinafter only the "NRA"), together with preparation of the Action Plan of the fight against legalization of proceeds from criminal activities and terrorist financing and financing of proliferation of weapons of mass destruction for 2019 – 2022 (hereinafter only the "Action Plan") in form of a non-legislative document which is to be submitted for approval by the Slovak Government in 2019.

From legislative point of view, the year under assessment brought another amendment of Act No. 297/2008 Coll. on the prevention of legalisation of proceeds of criminal activity and terrorist financing and on changes and amendment to certain acts, as amended (hereinafter only the "AML Act"). The main purpose of this, already the 12<sup>th</sup>, amendment of the AML Act was the transposition 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 purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (hereinafter only the "IV. AML Directive"), responding to recommendations of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (hereinafter only the "Moneyval Committee") and recommendations of the Financial Action Task Force (hereinafter only the "FATF"), with the aim to effectively respond to the ongoing developments in the area of fight against money laundering and terrorist financing.

### 1. Financial Intelligence Unit

FIU is the only national central authority in the area of prevention of the use of the financial system for the purposes of money laundering or terrorist financing. As a specialised unit of the Police Force (hereinafter only the "PF") it reports to the Presidium of the PF and forms an integral part of the National Criminal Agency of the Presidium of the PF (hereinafter only the "NAKA"). FIU is comprised of four divisions:

- Unusual Business Transactions Division,
- Obligated Entities Control Division (hereinafter only the "OEC"),
- International Cooperation Division, and
- Analyses Division.

FIU is also a part of the global network of financial intelligence units, the purpose of which is to apply international FATF standards FATF in fight against money-laundering and terrorist financing.

The legislative framework for the FIU's activities is comprised mainly of the AML Act, the National Council of the Slovak Republic Act No. 171/1998 Coll. on the Police Force, as amended (hereinafter only the "PF Act"), Act No. 199/2004 Coll. on the Customs Act and on changes and amendments to certain acts, as amended (hereinafter only the "Customs Act"), legal regulations of the European Union and

international treaties to which the SR has acceded (in particular the Vienna Convention, the Warsaw Convention and the Palermo Convention).

## 2. Unusual business transactions

The FIU's key task is to accept, analyse, assess and process reporting of unusual business transactions (hereinafter only the "UBT"), which is preceded by reporting duty of the obliged entities defined by law, in particular banks and other financial institutions and non-financial institutions (Art. 5 of the AML Act). Legal definition of UBT and demonstrative list of UBTs are in Art. 4 of the AML Act.

After receiving a notification of UBT, analysis is performed and, as a part thereof, the obtained information is supplemented in accordance with the AML Act and the PF Act. Depending on the facts of the case the reported information about an UBT is forwarded to:

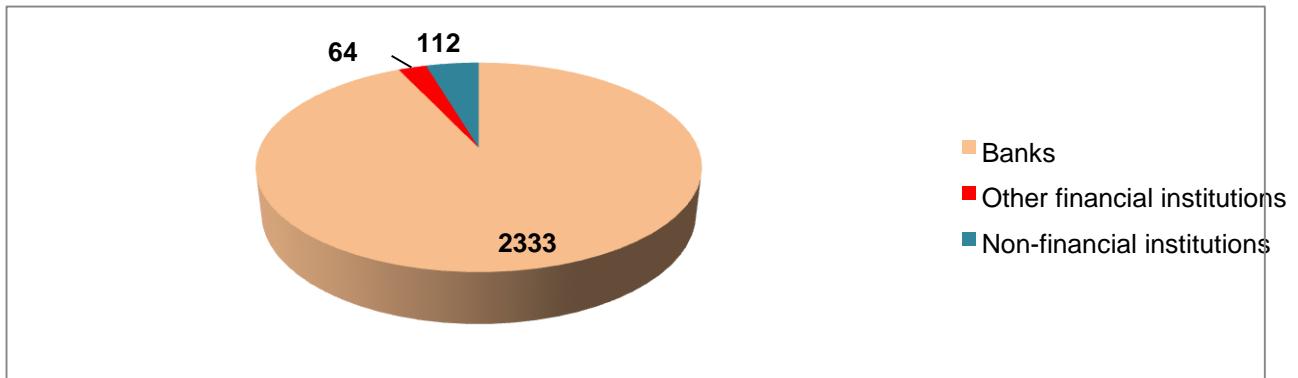
- Authorities acting in criminal proceedings (hereinafter only the "AACP") if the facts resulting from UBT notifications indicate that a criminal offence was committed, or that performance of the UBT may result in committing a criminal act and that it may make it impossible to seize the proceeds of criminal activities or complicate seizure thereof, or that the examined information does not relate to the already pending criminal proceedings, however, can be important for such proceedings;
- PF units, in particular, the Criminal and Financial Police Service for performance of responsibilities in accordance with the PF Act, including information about persons examined for suspicion of committing other criminal activities falling under their competence;
- The tax administrator (centrally: Financial Directorate SR, hereinafter only the "FD SR"), if the analysis reveals that the information give reason to commence tax proceedings or may be of importance of already pending tax proceedings,
- Competent units of member states of the member states of the European Union, in particular partner foreign intelligence units (hereinafter only the „FIU“) if the information include any international aspects which may be relevant for that FIU in terms of suspicion of a predicative criminal act or legalization of proceeds from criminal activities and terrorist financing;
- OEC Division, if, examination of the UBT notification revealed that an obliged entity fails to comply or is in breach of obligations imposed by the AML Act.

If an examination of an UBT notification does not reveal any fact which would be a reason to forward the information to the above mentioned entities, the information is entered in the knowledge fund of the FIU's Comprehensive Information System (hereinafter only the "CIS") for further use during investigation of other cases.

In 2018, FIU received altogether 2509 UBT notifications from obliged entities concerning total amount of EUR 1,350,869,599.00. Considering the type of the obliged entity, UBT notifications can be divided into three basic groups:

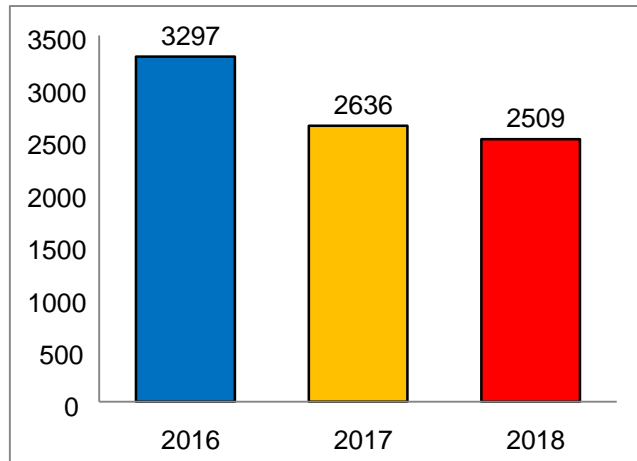
- UBT notifications received from banks operating in the territory of the SR including the National Bank of Slovakia (hereinafter only the "NBS") - altogether 2333 notifications,
- UBT notifications received from other financial institutions other than banks - altogether 64 notifications,
- UBT notifications received from non-financial institutions - altogether 112 notifications.

Chart No.1 Total number of UBT notifications received in 2018



Source: Statistical data FIU

Chart No. 2: Dynamics of the number of UBT notifications received in 2016 – 2018



Source: Statistical data FIU

Table No. 1: Number of UBT notifications received in 2016 - 2018 from banks

Banks operating in the territory of Slovakia			
Obligated entity	Number of UBT notifications		
	2018	2017	2016
NBS	53	59	79
Commercial banks operating in the SR	2280	2496	2994
<b>Total</b>	<b>2333</b>	<b>2555</b>	<b>3073</b>

Source: Statistical data FIU

Table No. 2: Number of UBT notifications received in 2018 from other financial institutions

Other financial institutions	
Obligated entity	Number of UBT notifications
Central Securities Depository, securities trader	6
Insurance company	14
Pension management company	1
Supplementary pension management company	5
Legal entity or a natural person authorised to perform auctions, excl. executions, finance leases or other financial institution	9
Payment institution	24
Custodian and depository	5
<b>Total</b>	<b>64</b>

Source: Statistical data FIU

Table No. 3: Number of UBT notifications received in 2018 from non-financial institutions

Non-financial institutions	
Obligated entity	Number of UBT notifications
Operator of hazardous games	106
Postal services provider	2
Attorney at law or notary	4
<b>Total</b>	<b>112</b>

Source: Statistical data FIU

From among 2509 received UBT notifications, 824 sets of information were entered in the knowledge funds for further convenience. After a thorough analysis of the received UBT notifications, processing thereof and subsequent evaluation, and considering the conclusion as to which of the information may be relevant for specific entities, the FIU provided in particular:

- 252 sets of information to the AACP,
- 295 sets of information to NCS national units, thereof 60 sets of information to the national counterterrorism unit of the NCA,
- 313 sets of information to regional and district PF Directorates,
- 980 sets of information to the FD SR,
- 2 sets of information to the OEC Division,
- 374 sets of information to foreign FIUs.

The institute of postponement of an UBT in accordance with Art. 16 of the AML Act by the obliged entity is a serious legal action in an effective fight against legalization of proceeds from criminal activities, which is applied if performance of the UBT could make it impossible to seize the proceeds of criminal activities intended for terrorist financing or complicate seizure thereof.

In 2018 from among total number of received UBT notifications, postponed were 71 UBTs totalling EUR 4,017,793.52, thereof in one case upon request of a partner FIU and in one case upon the FIU's request. In 44 cases, information from the notifications were forwarded to competent AACP (based on their factual and venue authority) for further action in accordance with provisions of the Code of Criminal Procedure.

Table No. 4: Statistical overview of postponed UBTs for 2018

Total number of postponed UBTs	71
UBT postponed by the obliged entity	69
UBT postponed upon the FIU's request	1
UBT postponed upon request from a foreign FIU	1
Forwarding the postponed UBT to the competent AACP	44
Total amount of the postponed UBT	EUR 4,017,793.52

Source: Statistical data FIU

In 2018, in 298 cases, obliged entities refused to enter into a business relationship, terminated a business relationship or refused to carry out a transaction in accordance with Art. 15 of the AML Act; total amount of the transactions was EUR 51,147,046.00.

With respect to the information forwarded to the AACP, for 2018, the FIU's records show that 22 prosecutor's orders were issued to seize financial funds kept on bank accounts; total amount of the seized financial funds was EUR 1,024,951.00.

In accordance with the AML Act, FIU informs the obliged entity about effectiveness of UBT notifications and procedures following receipt of the notification. For that purpose, FIU requires from AACP information (feedback) about results of the examination of the received information and further steps taken in this matter. As obtaining of the feedback (numbers of commenced criminal proceedings, accusations brought, motions for accusation until conviction) is a dynamic process of a longer nature, there can be a difference in numerical values at the moment of obtaining statistical supporting documents for preparation of the Annual report, compared to certain time lapse. Considering the aforementioned facts, Table No. 5 provides a summary of procedures of the AACP with data updated for 2017 and 2016; the original values in Annual Reports are given in brackets.

Table No. 5: AACP's procedure after forwarding information under Art. 26 par.2 b) of the AML Act

<b>AACP's procedure after receiving information from FIU</b>	<b>Number of cases (2018)</b>	<b>Number of cases (2017)</b>	<b>Number of cases (2016)</b>
Commencement of criminal prosecution under Art. 199 of the Code of Criminal Procedure – in all cases	47	78	58 (52)
Commencement of criminal prosecution under Art. 199 of the Code of Criminal Procedure for criminal act of legalization of proceeds of criminal activities under Art. 233 and 234 of the Criminal Code	33	52	29 (25)
Commencement of criminal prosecution under Art. 199 of the Code of Criminal Procedure – for other criminal act	14	26	29 (30)
Accusation under Art. 206 of the Code of Criminal Procedure for criminal act of legalization of proceeds of criminal activities under Art. 233 and 234 of the Criminal Code	1	3 (0)	2 (0)
Accusation under Art. 206 of the Code of Criminal Procedure - for other criminal acts	6	4 (2)	1 (0)
Discontinuation of criminal prosecution under Art. 215 of the Code of Criminal Procedure	0	1	2 (1)
Refusal to start criminal prosecution under Art. 197 par. 1 d) of the Code of Criminal Procedure	11	20 (19)	10 (7)
Seizure of financial funds under Art. 95 of the Code of Criminal Procedure	22	20	30

Source: Statistical data FIU

In 2018, the FIU's records show seven cases when an accusation was brought under Art. 206 of the Code of Criminal Procedure; in one case, accusation was brought against a person for criminal act of legalization of proceeds from criminal activities under Art. 233 of the Criminal Code, further cases involve criminal act of fraud under Art. 221 of the Criminal Code. Two of the above-mentioned seven cases, include a motion for accusation under Art. 209 of the Code of Criminal Procedure criminal act of fraud under Art. 221 of the Criminal Code.

The data provided to the FIU by the PF of the Ministry of Interior SR (MI SR), the Criminal Office of the Financial Administration (COFA), from the criminal division of the General Prosecution SR (GP SR), the Special Prosecution Office (SPO GP SR) and the Ministry of Justice SR (MS SR), were used by the FIU to prepare an integral statistical output on the overall number of motions for criminal prosecution, commencement of criminal prosecution, accusation, methods of termination of criminal prosecution, number of identified, prosecuted, accused and convicted persons in case of legalization of proceeds from criminal activities and in case of terrorist financing, as summarized in Table No. 6.

The supporting documents provided by PF divisions show that in 2018, NCA initiated two presently pending criminal proceedings for terrorist financing under Art. 419c of the Criminal Code. In 2018, other public authorities did not report any cases of motions for criminal prosecution, commencement of criminal prosecution, accusation, legal action brought or final judgement rendered for the above mentioned criminal acts.

Table No. 6: Statistical data on criminal acts of money laundering under Art. 233 and 234 of the Criminal Code and terrorist financing under Art. 419c of the Criminal Code

Provision of the Code of Criminal Procedure	MI SR									GP SR						MJ SR						COFA									
	2018			2017			2016			2018		2017		2016		2018			2017			2016									
	Number of assets	Persons	Loss in EUR	Number of assets	Persons	Loss in EUR	Number of assets	Persons	Loss in EUR	Number of assets	Persons	Number of offences	Persons	Loss in EUR	Number of offences	Persons	Loss in EUR	Number of offences	Persons	Loss in EUR	Number of offences	Persons	Loss in EUR	Number of offences	Persons	Loss in EUR	Number of offences	Persons	Loss in EUR		
1. Motion for crim. prosecution	40	42	688.287	33	47	34.844.038	41	54	868.019	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	0	0	0	1	0	85.950
2. Art. 199 Starting crim. prosecution	95	x	33.387.198	91	x	38.686.978	111	x	13.874.895	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	1	1	85.950	1	0	85.950
3. Art. 206 Accusation	45	46	12.528.960	13	75	144.182.829	17	20	750.267	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	0	0	0	0	0	0
4. Art.209 Termination of investigation (accelerated investigation) of NPO	7	9	3.150.734	7	7	104.265	11	20	3.925.422	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	0	0	0	0	0	0
5. Suspension of criminal prosecution Art.215	8	3	280.822	7	5	234.000	6	2	53.558	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	0	0	0	0	0	0
6. Art. 228 par. 1, 2 Discontinuation of criminal prosecution	32	12	11.684.573	32	9	4.863.397	45	16	5.562.890	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	0	0	0	0	0	0
7. Art. 228 par. 5 Continuation of criminal prosecution	5	4	1.017.529	5	2	725.196	11	6	281.392	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0	0	0	0	0	0	0	0
8. Art. 233, 234 Accusation	-	-	-	-	-	-	-	-	-	*	20	*	82	24	42	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
9. Art. 331 Guilt & punishment agreement	-	-	-	-	-	-	-	-	-	*	0	*	13	3	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
10. Art. 284 Judgment (final)	-	-	-	-	-	-	-	-	-	*	25	*	28	14	18	11	22	x	-	12	121.956	-	18	737.205	-	-	-	-	-	-	

Source: Statistical data from divisions of PF MI SR, GP SR (Criminal Division GP SR + SPO GP SR), MJ SR, COFA

\* Criminal Division of the GP SR keeps statistical data for completed criminal prosecution cases, therefore, it is impossible to quantify number of assets or cases for the GP SR.



The analysis of UBT notifications shows that in 2018, the most frequently occurred cases of legalization of proceeds from criminal activities and associating thereof with predicative criminal activities included:

- 1) Frauds, in particular so-called CEO frauds, internet frauds, but also fraudulent activities (phishing) and variations thereof (such cases have been forwarded to the competent AACP).

CEO frauds show a mildly growing trend; the frauds consisted in diverting payments, which, as a rule, included hacking e-mail communication between trading partner companies. The business partner who is to pay for goods, is in good faith informed of a change in payment details of the other business partner through a fraudulent e-mail, showing a high level of authenticity. The payment for the goods is then redirected to an account established for that purpose with a bank operating, as a rule, in a country other than the one where the business relationship is dislocated. Financial funds from such accounts are further transferred to bank accounts established in third countries or the transfers are immediately followed by cash withdrawals made through dummies. Less frequent were cases when accounts were kept with banks domiciled in the UK and there are indications that the accounts are established for persons who, as migrants from third countries, were granted asylum in the UK and now are used by criminal offenders as so-called 'white horses' (dummies).

The reported cases show that majority of persons who controlled and were authorised to dispose of the accounts prepared for receiving the "diverted cash", were both Slovak nationals and foreigners (in particular Hungarians and Italians), in cooperation with other offenders of various nationality and business companies seated in Hungary. The aggrieved companies were mostly business companies based in France, Denmark, Finland etc.

In 2019, number of CEO frauds is expected to grow as there are no preventive measures to restrict the same. Such frauds can only be prevented by consistent and ongoing verification of data presented in documents used for conduct of business relationship between two business partners.

Another major group of notified UBTs, however with a declining trend in occurrence, are internet frauds involving pretended sale of consumer goods, passenger cars, electronics and various industrial equipment. The pretended sale requested making an advance payment or the whole amount of the purchase price to a prepared account abroad, however no goods were supplied by the seller.

- 2) A notable part of the reported UBTs involved latent tax criminal offences. Another significant factors used in tax criminal activities included:
  - Involvement of fictitious and shell companies in complex business schemes and carousel chains aiming to cover the committed tax criminal offences, resulting in optimizing costs aiming to reduce the tax base, and to affect payments of VAT refunds for certain companies operating within the chain,
  - Registered offices of the companies are at addresses used as a virtual office; the bodies of Slovak companies are often comprised of persons of various nationality and the rights to dispose of the company's accounts are often granted to such persons,
  - Preference given to chain non-cash transfers made via internet banking in combination with cash withdrawals and/or deposits using third persons - so-called 'white horses', the purpose of which is to complicate identification of the origin of the cash upon entering the carousel, and also to complicate identification of origin of further cash flows in case of final cash transactions in the carousel,

- Using business accounts of Slovak and foreign legal entities for transit of financial funds through the Slovak Republic,
  - Making use of tax havens and offshore companies for placement of proceeds from criminal activities.
- 3) Making use of gambling accounts and anonymous prepaid cards (*paysafecard*) followed by transfer of financial funds from the gambling account to personal account without participation in the game.

This scheme of transactions between gambling accounts makes it possible to use gambling accounts to develop legal framework in transactions with financial funds which come from anonymous payment channels without proving the origin of the funds. The financial funds were then paid out to owners of the gambling accounts to bank accounts and the transfers were followed by cash withdrawals. Most of such reported UBTs involved notification of termination of the business relationship with owners of the gambling accounts. Indicators of potential legalization upon the reported UBT are: using the gambling account by persons other than the establisher of the gambling account, as the online games are played using the same IP address,

- The ultimate beneficiary of the gambling account and of the participation in the gambling may be unknown persons other than the player registered as the owner of the gambling account,
- Charging the gambling account, e.g., via PAYSAFECARD, i.e. using prepaid cards which can be purchased without the buyer's identification with the dealers in the SR and abroad, or via internet,
- Participation in a gambling game usually results in winning an amount equal to the deposit, and/or even in case of high probability of winning, the players give up their chance to win and proceed so as to facilitate recovery of the deposit,
- Payment of the winning to bank account.

#### 4) Transactions carried out using Bitcoin virtual currency

The cases of trading with bitcoins were reported by obliged entities mostly because, in fact, there is not possibility to verify trading with this virtual currency. The notifications also included description of specific transactions – purchase of the currency, which, at the beginning indicated that one of the business partners might have incurred an injury, however, owing to anonymous trading through virtual platforms it was impossible to ensure supporting documents and information to confirm the assumption. The virtual currency and, in particular, Bitcoin is no longer a national currency in EU countries and also is not supervised or regulated by the NBS.

In 2018, thanks to newly identified methods, we noted a number of cases when personal accounts were established by Slovak nationals (including account for minor persons), and then payments from abroad in hundreds/thousands of EUR were directed to those accounts and thereafter withdrawn in cash using payment cards from ATMs located in Benin, Africa. Credit payments from abroad were declared with description as an agency fee, fee for loan, commission, contribution, donation, assistance, etc. and clients – Slovak nationals stated that they sent payment cards to the established accounts abroad via courier service, and they often were unable to give a clear response (explain details about the purpose of opening the account, operations on the account, payments from abroad, withdrawals in Benin, etc.).

The payments received by Slovak nationals from abroad included payments which have been later identified as fraudulent. In detected cases, the involved clients - Slovak nationals were socially and economically disadvantaged individuals, or aged persons, their communication with the bank often showed their lack of orientation in the related issues. Those facts could indicate that this was a similar

system illegal eliciting of financial funds, as the so-called “Nigerian letters” detected in the past. The FIU detected several cases of such foreign payments, and then, before the final cash withdrawal from an ATM in Benin, the financial funds were transferred between personal accounts of the persons, most probably with the aim of obfuscation of the cash flows and complication of efforts to trace the origin of the funds.

Table No. 7: Statistical overview of the most often UBT in 2018

Type of UBT	Number of reported UBTs	Value of the transaction in EUR
Non-cash payments	1886	1 160 982 480
Cash transactions	1243	306 748 679,5
Foreign payments	1105	822 071 764
UBT with an “offshore” element	67	102 560 059
CEO fraud	95	10 797 881
Phishing	22	1 784 251
Insurance	14	827 437
Real estate	48	20 357 840
Internet fraud	40	376 407
Counterfeit securities	2	27 670 000
Gambling	108	3 546 789

Source: Statistical data FIU

## 2.1. Selected cases of UBT treatment

### *“Financial Agent”*

In November 2018, FIU received an UBT notification from Bank A, an obliged entity, regarding operations at Person B’s personal account, in particular recurring credit non-cash payments amounting to hundreds/thousands of EUR from various personal accounts, which were then followed by cash withdrawals, or gambling-related payments (slot gaming machines). During September and October 2018 credits amounted to EUR 36,720.00. When performing the client due diligence procedures, the bank employees found out that Person B provides financial agency services to Company C as a subordinate financial agent and uses its personal account for receiving deposits on the signed insurance policies. Pursuant to the bank statement person B was performing the activities on its account for a longer period.

In this regard, the FIU addressed Company C, which said that the variable symbols of the collected payments received to the Person B’s personal account are similar to numbers of their draft insurance policies and admitted similarities with their coding, however, were unable to either confirm or deny whether the numbers refer to their clients. Under the signed contracts, the subordinate financial agent (i.e., including Person B) are not authorised to accept premium payments from clients, i.e., they are not authorised to collect insurance premium.

Further investigation revealed that Person B under the name of Company C used counterfeited forms to sign agency contracts on investing financial funds and they had the elicited financial funds transferred to their personal account although they knew that they are unable to provide the clients with the promised interest payments or to repay the invested financial funds, and thus created so-called pyramid investing scheme without actual adding value to the financial funds.

FIU forwarded the information to the competent AACP, which commenced criminal proceedings for suspected fraud. Pursuant to Person B, total amount of the loss incurred was approximately EUR 400,000.00, and the loss documented by the AACP amounted to EUR 189,100.00 EUR.

### *“CEO Fraud 1”*

In January 2018 FIU received an UBT notification from Bank A, an obliged entity regarding two fraudulent payments received from two foreign companies B and C from accounts kept in Germany, totalling EUR 178,000.00. Each of the two foreign payments were made in equal amounts EUR 89,000.00 and were credited to the same amount kept by Bank A for Person D. A foreign bank applied for repayment of the financial funds back to foreign accounts of B and C companies, owing to fraud and sent a copy of the complaint. As the bank learned about the fraudulent payments in time, before disposal of the financial funds, adopted technical measures at the Person D's account and after the attempt to dispose of the financial funds at the Person D's account via Internet banking service then proceeded with postponement in accordance with Art. 16 of the AML Act.

Analysis of UBT notifications revealed that the transfers of the two above-mentioned foreign payments from foreign accounts were preceded by “hacking” the electronic business communication of the owner of the foreign accounts of B and C entities and the original payments were redirected to an incorrect account owned by Person D.

FIU then processed the information and forwarded it to the competent AACP, which, based on that information, commenced criminal prosecution for an attempt of a particularly serious crime of money laundering. The prosecution office then seized the financial funds on the Person D's account in total amount of EUR 178,000.00.

### *“CEO Fraud 2 with subsequent legalization”*

At the end of 2017 and at the beginning of 2018, FIU received several UBT notifications from one obliged entity - Bank A regarding CEO frauds followed by legalization of proceeds from such criminal activities. The criminal activities involved bank accounts of several persons kept with various branches of the same obliged entity - Bank A.

In the above mentioned cases, committed were partial attacks of a continuing criminal offence of money laundering. In all cases reported in notifications sent by the obliged entity - Bank A, the modus operandi was identical – a number of persons established bank accounts with Bank A, we receiving financial funds to those accounts exclusively from foreign bank accounts (from e.g., China, the Czech Republic, Saudi Arabia, UK, Turkey, Federal Republic of Germany, Switzerland, Lithuania, India, Spain, Morocco). The financial funds came from CEO frauds, which was obvious from the foreign banks' requests for payback of the financial funds. In accordance with Art. 16 of the AML Act, a part of the financial funds credited to Bank A's bank accounts were postponed and/or subsequently seized by AACP, however, majority of the funds was further transferred, in particular to further foreign bank accounts was further transferred to other foreign bank accounts, or were withdrawn in cash, and a part of the credited funds was, by return, sent back by Bank A to the sender's accounts immediately after the amount was credited (or before it was credited).

Total amount of the financial funds credited, and/or directed to Slovak bank accounts established by third parties from abroad (including the funds paid back to the senders) amounted to EUR 1,119,260.27 EUR.

In the above described cases, the FIU processed a number of facts which were then forwarded to the competent AACP and based on the information the AACP joined the partial proceedings and commenced criminal prosecution for particularly serious crime of legalization of proceeds from criminal activities. Then the AACP accused the offender B of particularly serious crime of legalization of proceeds from criminal activities committed in complicity. The investigation by the AACP revealed that offender B, either himself, however, mostly acting through other persons (agents) contacted other individuals, who

were then asked to establish a bank account with Bank A and were promised a reward for doing so (not more than several tens of EUR). After opening the account, the individuals (either directly, however mostly through third parties acting as agents) disclosed the internet banking access data and handed over the payment cards to the newly established account to offender B, and thus offender B could freely dispose of the accounts.

#### *Africa – misuse of a payment card*

In February 2018, FIU received an UBT notification from an obliged entity - Bank A; the e-mail notified Bank A of potentially fraudulent activities with respect to an account owned by person B.

Consequently, Bank A asked Person B to explain the origin of financial funds credited to Person B's account from countries of the European Union (hereinafter only the "EU"), and the withdrawals from the account made by payment card in Benin, Africa, mostly on town named Calavi.

As to the payments, Person B explained that he asked an unknown person C via internet for a borrowing and that lost the payment card. The card number and the number of the bank account were disclosed by Person B to Person C who granted the loan. Based on that information, Bank A blocked the Person B's payment card.

During the period from opening the account in 2017, altogether 140 credit payments were received to the Person B's account totalling EUR 59,021.00, in particular from the Netherlands (39 payments), Italy (11 payments), Germany (10 payments), but also from Slovakia (29 payments) and the Czech Republic (15 payments). Debit transactions by the payment card were made in total amount EUR 61,544.00 (169 cash withdrawals). Most of the cash withdrawals by the payment card in Benin were approved (the withdrawals were made) and the card holder entered the correct PIN code. No complaints from the transferor or a request for payback of any or the paid amounts were received by Bank A with respect to the amounts credited to the Person B's account.

Bank A then reviewed its system and detected other persons receiving payments from various entities to their accounts. The financial funds were then also withdrawn in cash in Calavi, Benin and no complaints have been filed with respect to the credited amounts.

The FIU prepared a comprehensive information thereof and forwarded it to the competent AACCP and the authority then commenced criminal proceedings for the offence of legalization of proceeds from criminal activities.

## **2.2. Forecast of further developments in money laundering and terrorist financing**

Based on analysis of the existing development trends in legalization of proceeds from criminal activities and terrorist financing and considering the obtained information, the existing facts and the latest events in the Slovak Republic, in the near future, it can be expected that income will be generated by:

- Property criminal activities similar to internet frauds and CEO frauds,
- Various, including new, forms of tax criminal activities,
- Using tax havens and offshore companies and involving shell and fictitious companies in complex business schemes;

- Using gambling accounts to create a legal title to prove the origin of financial funds;
- Misusing virtual currency trading.

### 3. Control and legislative activities

As a part of the FIU's internal organization, the OEC Division controls performance of responsibilities and compliance with responsibilities resulting for obliged entities from the AML Act.

In 2018, control activities were made, in particular, in accordance with the control plan for 2018. The categories of obliged entities in the control plan were proposed based on the risk-oriented approach, in particular from facts and information learned during previous controls of obliged entities, based on initiatives and information received from other PF units, knowledge of various irregularities and incompliances detected in preparation of UBT notifications.

The Control Plan for 2018 also took account of facts obtained with respect to performance of the NRA and relevant initiatives obtained from natural persons and legal entities.

During performance of the control, the OEC staff were focused on examination of proper performance of the client care, assessment of business transaction, UBT postponement and notification, and application of the "Know Your Customer" principle, i.e., obtaining sufficient amount of information about the nature of the client's expected transactions and any predictable scheme in financial operations carried out by the client.

In 2018, altogether ten controls were performed and the proportion between clients from the financial and non-financial sectors was 1:1. In five cases, administrative proceedings were initiated for a breach of the AML Act and fines were imposed in total amount of EUR 27,500.00. In three cases no incompliance was detected and in two cases no decision on the merits has been rendered.

Additionally, the OEC Division performed activities aimed at achieving final completion of proceedings in five controls started in 2017.

Table No. 9: Statistic data about number of controls, number and value of imposed fines in 2016 through 2018

Year	Number of controls	Outcome of the controls			Value of fines in EUR
		No sanction	Sanction	Pending	
2016	6	0	6	0	41 600
2017	5	0	5	0	49 200
2018	10	3	5	2	27 500

Source: Statistical data FIU

The most common findings from control activities performed by the OEC Division, with reference to provisions of the AML Act, included: incomplete or insufficiently prepared own action plan by obliged entities (Art. 20 par. 1 and 2), failure to provide necessary cooperation for control purposes (Art. 30 par. 1 through 3), failure to carry out proper client care procedures in accordance with Art. 10 of the AML Act (insufficient identification of the client and verification of data in the scope as required in Art. 7 and Art. 8, failure to identify the purpose and the planned nature of the business relationship, a failure to identify the ultimate benefit owner and the origin of the financial funds), failure to perform enhanced client care procedures (Art. 12), failure to assess business transactions under Art. 14 par. 2 of the AML Act, and failure to report an UBT under Art. 17 of the AML Act.

Within their methodological activities, the OEC Division presented their comments on practical application of the AML Act by entities classified as obliged entities under Art. 5 of the AML Act, based on a written (qualified) request, details of which are available at the FIU's website. In 2018, OEC Division prepared 12 comments.

Activities of the OEC Division further included various trainings, consulting or discussions focused on a number of application problems which occurred in relation to performance of the FIU's responsibilities under the AML Act. In 2018, the OEC Division attended various working meetings with respect to legislative procedures aimed at amendment of the AML Act in cooperation with the Security Legislation Dpt. of the Office of the Minister of Interior SR. In this regard, the OEC Division also attended sessions of the Constitutional and Legal Affairs Committee of the National Council of the SR (hereinafter only the „NC SR“), the Economic Affairs Committee of the NC SR, Financial and Budgetary Committee of the NC SR, Defence and Security Committee of the NC SR, and the session of the NC SR.

In its letter addressed to chambers, associations and trade associations, the OEC Division informed the obliged entities of enactment of Act No. 52/2018 Coll., amending the AML Act, highlighting the most important changes in the Act.

In relation to completion of the NRA process, results of the assessment for securities, banking and insurance sectors were presented in form of lectures at personal meetings with obliged persons.

The OEC Division also facilitated the legislative procedures related to submitting the Action Plan as a non-legislative legal act for discussion by the Government of the SR.

In relation to transposition of the amendment of the IV. AML Directive, the OEC Division attended discussions with representatives of the Security Legislation Dpt. of the Office of the Minister of Interior SR, Ministry of Finance of the SR and NBS representatives.

Table No. 10: Summary of activities of the OEC Division

Obliged entity (trade association) which was subject to the activity	Subject matter of the training, discussion, consulting
Institute of Banking Education/ Slovak Banking Association / banks	Problems in application of the AML Act, preparation of UBT notifications for the FIU, presentation of NRA results for the banking module.
Insurance companies and insurance agents	Problems in application of the AML Act, presentation of NRA results, trainings and consulting related to amendment of the AML Act
Securities traders	Presentation of NRA results for securities module, trainings and consulting related to amendment of the AML Act
Slovak Chamber of Auditors	Training followed by consulting on amendment of the AML Act
Chamber of Notaries of Slovak Republic	Training followed by consulting on amendment of the AML Act
Post Office Company	Training followed by consulting on amendment of the AML Act

Source: Statistical data FIU

## 4. International cooperation

Sharing financial intelligence information is of paramount importance and became the cornerstone of the international effort in the fight against money laundering and terrorist financing. It means that money laundering and terrorist financing can only be addressed by joint effort on both national and international levels. Pursuant to international AML and TF standards, FIUs all around the world shall share their information and join international cooperation.

The FIU invests in maintenance and extension of international cooperation with its peers not only in the operative exchange of information, but also in transfer and exchange of knowledge and experience. FIU is an active member of international bodies, such as Moneyval, Egmont Group, FIU.NET and FIU Platform within the EU.

### 4.1. Forms of cooperation

International cooperation is not limited to specific cases only, but also includes a general exchange of experience, best practice and participation in international working groups and organizations.

The exchange of information in global context is governed by national legal regulations which are based on the information exchange principles of the FIU Egmont Group. It is a platform for safe exchange of professional knowledge of financial information intended primarily for the fight against legalization of proceeds from criminal activities and terrorist financing. FIU has been a member of the Egmont Group since 1997. As a global association of national FIUs, the Group is presently comprised of 158 FIUs.

### 4.2. Methods of international communication and evaluation of cooperation with partners on the international level

In practice, information between members of the Egmont Group is exchanged through a secured and enciphered electronic information-sharing network Egmont Secure Web (ESW), allowing to communicate with FIUs from all around the world. Another option is communication via Financial Intelligence Unit Network (FIU.NET). It is a decentralized computer network allowing exchange of information between FIUs based in member states of the European Union. A sophisticated technology Ma3tch has been developed under FIU.NET allowing FIUs connected to FIU.NET, to anonymously compare whether their data are in line with those shared by other FIUs.

Table No. 11: Summary of selected activities of the International Cooperation Dpt. in 2016 – 2018

Year	Number of requests sent abroad	Number of settled requests from abroad	Number of notices forwarded abroad*	Number of notices about Slovak entities received from abroad
2016	78	321	321	156
2017	89	265	654	211
2018	85	240	555	420

Source: Statistical data OMS FIU

\* "The number of notices forwarded to foreign FIUs includes overall number of forwarded noticed, not only information learned from UBT notifications (e.g. supplementary information, information resulting from own activities, etc.)."



If requests from abroad meet the minimum requirements defined in the Egmont Group principles for exchange of information, (e.g., relevance to the addressed country, sufficient reasons for suspicion of money laundering or terrorist financing, detailed description of the case), the FIU can share the available information with partner FIUs from abroad. The shared information can then be used solely for analytical or intelligence purposes for further operative investigation. The information cannot be further forwarded to AACP, unless an explicit approval is received from the sending FIU. If the information appears to be of useful and need to be used as an evidence in criminal proceedings, a request shall be filed through international legal assistance.

On a bilateral level the FIU was focused on cooperation regarding individual specific cases. The countries which most frequently asked the FIU for information in 2018 through ESW and FIU.NET networks included: the Czech Republic (49), Hungary (44), Italy (25), Germany (11), Ukraine (12), USA (8), France (8), the UK (6) and Estonia (6). On the other side, the countries whom FIU sent requests for information in 2018 through ESW and FIU.NET networks included in particular: Germany (12), the UK (11), the Czech Republic (9), Hungary (4). Under the available statistical information obtained from the headquarters of FIU.NET Bureau, regarding the requests sent and inquiries received through FIU.NET communication network, in 2018 the FIU ranked 12th among 28 involved FIUs.

In the reporting period FIU altogether sent through FIU.NET and ESW 555 unsolicited notices (thereof 135 through ESW and 417 through FIU.NET). Most of the notices were forwarded to FIU Hungary (103), FIU Czech Republic (72), FIU Italy (44), FIU Poland (32), FIU Germany (27), FIU Austria (23), FIU UK (26), FIU Ukraine (21), FIU France (13) and FIU Switzerland (12).

Through the above-mentioned electronic systems (ESW and FIU.NET FIU) the FIU received altogether 420 unsolicited notices from foreign partner FIUs. The largest numbers of notices were received from FIU Czech Republic (59), FIU Hungary (25), FIU Germany (12), FIU Austria (8), FIU Slovenia (9) and FIU Croatia (7).

Considering the international nature of money-laundering, in particular in neighbouring countries, the FIU understands the necessity of enhancing the cooperation with the partner FIUs, in particular in the neighbouring countries, and to improve own knowledge in the fight against legalization of proceeds from criminal activities and terrorist financing by making use of information and experience shared by the closest partner, as the direct cooperation of stakeholders in this area and prompt coordination of activities is the basis for an effective progress in facing this challenge. That is one of the reasons for regional workshops organised on an annual basis to encourage a solid international cooperation between neighbouring partner FIUs in Austria, Czech Republic, Hungary, Poland, Slovenia and the Slovak Republic, which are regularly attended by selected representatives of FIUs from all the above-mentioned countries. In 2018, the workshop was organised by FIU Hungary and the key topics discussed by the participants included: use of FIUs in the fight against tax frauds in relation to AML, discussion on the latest urgent issue – crypto currency and experience of the present FIUs with this phenomenon in analysing UBT notifications, FIUs' strategic analyses, impacts of the new EU legislation on national legislation.

#### **4.3. FIU's representation at international organizations**

##### *Moneyval Committee*

In 2018, representatives of the FIU attended three plenary meetings of Moneyval in Strasbourg. One of those plenary meetings discussed the follow-up report of the SR on elimination of irregularities

identified during the 4<sup>th</sup> evaluation visit of the Moneyval Committee in 2010. As Slovakia officially started the 5<sup>th</sup> round of mutual evaluation of member states of the Council of Europe by the Moneyval Committee, in view of Slovakia, the 4<sup>th</sup> round has been completed and all insufficiently met recommendations will be given even more attention by the evaluators in the 5<sup>th</sup> round. With respect to the commenced 5<sup>th</sup> round of evaluation.

#### *Expert Group for Fight against Money Laundering and Terrorist Financing (EGMLTF) and FIU Platform*

In 2018, representatives of the FIU attended regular meetings of the *Expert Group for Fight against Money Laundering and Terrorist Financing* in Brussels (EGMLTF) and meetings of the FIU Platform, which is an informal association of FIUs from EU member states, established in 2006 by the European Commission. The main purpose for establishing the FIU Platform was to facilitate the cooperation between FIUs and to provide the European Commission with consulting and expert knowledge in FIU-related issues. The subject matter of negotiation of these countries were, in particular, irregularities of EU member states in implementation of the 4<sup>th</sup> AML Directive and transposition of the amendment of the 4<sup>th</sup> AML Directive by EU member states, the prepared Directive on AACP's access to financial information and the prepared reporting of the European Commission on the International Risk Assessment, cooperation between FIUs within the EU and the list of high-risk third countries.

## **5. Cross-border notification**

Under the existing Customs Act, FIU is the only competent national authority receiving notifications of carried cash (hereinafter only the "Notification"), from individuals who, upon entering or leaving the EU from/to a country outside the Schengen area, declare that they carry cash in an amount equal or higher than EUR 10,000.00. The obliged entity (Art. 4 par. 2 of the Customs Act) is deemed to comply with the requirement if, upon crossing the external border, the prescribed form, properly completed and providing all obligatory details, is submitted to customs authorities. Under the existing law, the authorized forms are then sent by the customs authorities to the FIU (Art. 4 par. 4 of the Customs Act).

In 2018, the FIU received from Slovak customs authorities altogether 230 Notifications in total amount of EUR 8,131,825.21. From among the received Notifications, in 23 cases, on-the-spot fine was imposed owing to the failure to report the carried cash, the total amount of the imposed fines was EUR 2,030.00 (16 detected cases were reported by the Customs Office Bratislava Airport of M. R. Štefánik and 7 detected cases were reported by Vyšné Nemecké branch of the Customs Office). In 69 cases, the cash was transported by air, the rest were detected at the EU land border between the Slovak Republic and the Ukraine.

Under the existing Customs Act, obliged entities were mostly nationals from the Ukraine (111) – most of them were persons who were repeatedly crossing the external border and reported the carried cash. It was also found that when proving their identity upon crossing the external border, some of those persons once identified themselves as Ukraine nationals and at the following border crossing they filled in Hungarian nationality in the form), Hungary (22) and the Russian Federation (8), who were crossing the external border through the road border crossing Užhorod – Vyšné Nemecké (102), Mali Selmenci – Veľké Slemence (49), Malyj Bereznyj – Ubľa (10) and upon arrival to/departure from Airport of M. R. Štefánik in Bratislava (68) or Košice Airport (1).

The purposes of use of the carried cash most frequently declared by the obliged entities included: own savings intended for purchase of property (53), purchase of a motor vehicle (51), deposit to a bank account (47), business (28), personal use (22) and various purchases (19), and in most cases the Slovak

Republic was declared as the destination country. In certain cases, the Slovak Republic was just the transit country and the obliged entities mostly intended to spend the carried cash in the Czech Republic, Austria, Germany, Slovenia and Poland.

After verified in information systems available to the PF, including the CIS FIU, and open information sources, the information from received notifications were entered in the CIS FIU for further use (176). FIU proactively forwarded 40 notices to relevant FIUs for their further convenience; in 7 cases the information was forwarded to competent police authorities and in 19 cases the information from the notification was forwarded to the Financial Directorate SR for further use in tax proceedings.

Table No. 12: Overview of the number of notifications of cash carried from/to the EU received by the FIU and the amount of cash carried in years 2016 - 2018

Year	Number of received notifications	Amount of carried cash in EUR
2016	124	4,016,396.51
2017	152	5,261,245.86 + 1 bond of \$14,975,000,000
<b>2018</b>	<b>230</b>	<b>8,131,825.21</b>

Source: Statistical data of AD FIU

## 6. Evaluation of the cooperation with partner entities

The FIU's good quality and effective operation depends on the quality of coordination of activities of all authorities involved in the fight against legalization of proceeds from criminal activities and terrorist financing. In 2018, the coordination included two important activities and a number of liaison coordination meetings, in particular with key partners participating in fight against legalization of proceeds from criminal activities and terrorist financing on national level (other police units, Ministry of Finance SR, Ministry of Justice SR, GP SR, Ministry of Foreign and European Affairs SR, NBS, COFA, the Slovak Intelligence Service, Military Intelligence, etc.).

The first important activity was the meeting of members of the National Expert Group for prevention and fight against legalization of proceeds from criminal activities and terrorist financing (hereinafter only the NEG-ML). Unlike previous years, in 2018 activities of the NEG-ML were officially reduced, as only one meeting of the Group was held. Moreover, the agenda of the meeting did not discuss any typological issues or any interdepartmental issues related to the criminal activities. The major purpose of the meeting was to inform the members of the Group of the content of presentations intended for proving of effectiveness of implementation of 40 FATF recommendations for the purpose of the methodological and instructing workshop within the 5<sup>th</sup> round of evaluation of the Council of Europe member states by the Moneyval Committee. Members of the Group were familiarized with the content of eleven presentations on the Moneyval's immediate results, and that is the key point of evaluation in the 5<sup>th</sup> round of evaluation. Considering the horizontal nature of individual direct results, it is necessary that several departments and entities participate and cooperate in the preparation thereof. The presentations preceded the preparation to completion of Moneyval questionnaires.

With respect to the started 5<sup>th</sup> round of evaluation, the second key activity within cooperation and coordination on national level is organizing a two-day methodological and instructing workshop, which is based on FATF procedures. Approximately a year before the evaluation visit, the Moneyval Secretariate sends two trainers to the workshop for the country under evaluation, to use the FATF presentations

(prepared exclusively for this purpose) as the general introduction for the 5<sup>th</sup> round of evaluation, together with several modules referring to evaluation procedures. Then, presented are all immediate results, the key properties thereof, horizontal irregularities and best practices of countries, which already underwent the FATF/Moneyval evaluation.

The training for the SR was provided on 13<sup>th</sup> and 14<sup>th</sup> November 2018. Invited were major stakeholders from the public and the private sector, as they will participate in preparation of documents necessary for the evaluation (completion of questionnaires, personal meetings during the evaluation visit). Additionally, the trainings were attended by persons responsible for preparation of the NRA and implementation of findings resulting from the evaluation. The purpose of the training was to raise any issues which can be faced by competent entities during completion of the questionnaires or during the evaluation visit so that Moneyval Secretariate could provide the necessary guidance. The objective of the methodological and instructing workshop has been met.

## CONTACT DATA

### ADDRESS

Ministry of Interior of the Slovak Republic  
Presidium of the Police Force  
National Criminal Agency  
Financial Intelligence Unit  
Pribinova 2  
812 72 Bratislava

### INTERNET

web: [www.minv.sk/?financna-policia](http://www.minv.sk/?financna-policia)  
e-mail: [sjfpsek@minv.sk](mailto:sjfpsek@minv.sk)

### TELEPHONE/FAX

Tel.: 09610/51402  
Fax: 09610/59047

### CONTACT DATA for UBT NOTIFICATION

In person: Račianska 45, 832 02 Bratislava  
In writing: Financial Intelligence Unit, Pribinova 2, 812 72 Bratislava  
Electronic: [sjfpnoo@minv.sk](mailto:sjfpnoo@minv.sk)  
Tel.: 09610/51419  
Fax: 09610/59047