Ministerstwo
Finansów

NATIONAL ASSESSMENT OF THE RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Warsaw, 2019

TABLE OF CONTENTS

TABLE OF CONTENTS

Abbreviations and acronyms:

ABW	Internal Security Agency
AIF	alternative investment fund
AML/CTF	anti-money laundering and counter-terrorist financing
AIC	alternative investment company
ATS	Alternative Trading System
OPS	Office of Payment Services
CAT	ABW Counter-Terrorist Centre
CBA	Central Anti-Corruption Bureau
CBŚP	Central Bureau of Investigation of the Police
CPT ABW	ABW Terrorist Prevention Centre
CRBO	Central Register of Beneficial Owners
DFE	voluntary pension fund
GNI	gross national income
Dz. U.	Journal of Laws of the Republic of Poland
OJ EU	Official Journal of the European Union - OJ EU)
ECB	European Central Bank
EEA	European Economic Area
ESMA	European Securities and Markets Authority
ESW	*Egmont Secure Web*, i.e. the IT system developed within the Egmont Group and used by FIU being members of this Organisation
FATF	*Financial Action Task Force* (established in 1989 during the G-7 summit in Paris, dealing with the analysis and assessment of threats related to money laundering and financing of terrorism, in particular in the context of 40 recommendations it issued, defining international standards in the scope of counteracting money laundering and financing of terrorism and proliferation)
FIO	open-end investment fund
FIU.net	system of information exchange between financial intelligence units of EU member states
FIZ	closed-end investment fund
FTF	foreign terrorist fighters
GIFI	General Inspector of Financial Information
WSE	Warsaw Stock Exchange (Giełda Papierów Wartościowych w Warszawie S.A.)
GUS	Central Statistical Office
IBnGR	Institute for Studies on Market Economy
ICO	initial coin offerings

IDM	Chamber of Brokerage Houses
IPAG	Institute of Economic Forecasting and Analysis
ISIS	Islamic State of Iraq and Sham
IZFiA	Chamber of Fund and Asset Management
FIU	financial intelligence unit (in accordance with the FATF Recommendation no. 29 – the financial intelligence unit shall mean “a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis” which “should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly”)
KAS	National Revenue Administration
FSC	Financial Security Committee
KCIK	National Centre of Criminal Information
KDPW S.A.	National Depository of Securities (Krajowy Depozyt Papierów Wartościowych S.A.)
KGP	Police Headquarters
DPI	Domestic Payment Institution
kk	Penal Code
kks	Penal Fiscal Code
KNF (PFSA)	Polish Financial Supervision Authority
KRS	National Court Register
ksh	code of commercial companies
SPI	Small payment institutions
MONEYVAL	also referred to as the MONEYVAL Committee - *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*, (the body of the Council of Europe established in 1997 dedicated for the monitoring and assessment of MONEYVAL member states' compliance with the basic international rules related to AML/CTF, as well as effectiveness of their implementation, being a FATF-style regional body and a FATF affiliate member)
MVTS	*money or value transfer services*, i.e. financial services consisting of the acceptance of cash, cheques, other monetary instruments and values and making of payments of appropriate amounts in cash or in another form to a beneficiary of a transaction through various communication and settlement channels (this term also includes systems designated as *Hawala, hundi* and *fei-chen*)
NBP	National Bank of Poland (Narodowy Bank Polski)
NPO	non-profit organisation
NSA	Supreme Administrative Court

OECD	Organisation for Economic Co-operation and Development
OFE	open pension fund
OIC	Organisation of Islamic Cooperation
OTF	organised trading facilities, i.e. an organised trading platform other than a regulated market or an ATS
GDP	Gross Domestic Product
PrTE	Employee Pension Fund Companies
RP	Republic of Poland
RWE	right-wing extremist
SAR	Suspicious Activity Report
SFIO	specialised open-end investment fund
SG	Border Guard
SKOK	Cooperative Savings and Credit Union
SKW	Military Counter-Intelligence Service
SWW	Military Intelligence Service
STIR	ICT system of the clearing house, referred to in the provisions of Title IIIB - "Counteracting the use of the financial sector for tax fraud" *of the Act of 29 August 1997 - Tax Ordinance* (Journal of Laws of 2018, item 800 as amended)
STR	Suspicious Transaction Report
TFTP	Terrorist Finance Tracking Program
EU	European Union
UKE	Electronic Communications Authority
UKNF	Office of the Polish Financial Supervision Authority
VAT	value-added tax
WSA	Regional Administrative Court
ŻW	Military Police

1. INTRODUCTION

1. 13 July 2018 was an important date in the history of the Polish anti-money laundering and counter-terrorist financing system. On that date, the majority of the provisions of the Act of 1 March 2018 on *Counteracting Money Laundering and Financing of Terrorism* entered into force (Journal of Laws 2019, item 1115) changing the background of its operation. One of the innovations was the introduction of the provisions of Chapter 4 committing to the preparation of the national assessment of the risk of money laundering and financing of terrorism and its periodic updating.

2. In one of its recommendations, the Financial Action Task Force (FATF) indicated the need to identify and assess the risk of money laundering and financing of terrorism occurring in each country in order to ensure that the measures implemented to counteract these crimes are adequate to the identified risks in this area. The reference to the approach based on risk analysis defined in this way was also reflected in the European Union (EU) regulations which were implemented in the aforementioned Act.

3. The General Inspector of Financial Information (the GIFI), without waiting for the adoption of the aforementioned Act, as early as in 2016 started works on the preparation of the first national assessment of the risk of money laundering and financing of terrorism, simultaneously cooperating with the European Commission and its counterparts from other EU member states on the creation of the transnational assessment of the risk of money laundering and terrorist financing. Information on these works was presented in the annual reports on the GIFI activities published on the website of the Ministry of Finance. One of the first measures was the development of the draft methodology which is largely based on the methodology prepared for the supranational assessment of the risk of money laundering and financing of terrorism. The assumptions underlying the national assessments of the risk of money laundering and financing of terrorism prepared in other countries were also taken into account. The final version of the adopted methodology is presented in Annex 1 hereto.

4. While preparing the first national assessment of the risk of money laundering and financing of terrorism, a wide range of data and information from different areas, not necessarily directly relevant to counteracting of these crimes, was taken into consideration. Such a broad spectrum required the cooperation of many people with knowledge and experience, sometimes in very specialised areas. The *Working group for identification and analysis of information and documents in order to fulfil the obligation referred to in Article 26 of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, established at the beginning of 2019 at the Financial Security Committee, played an important role in the completion of the final version of the national assessment of the risk of money laundering and financing of terrorism. External experts also took an active part in its works.

2. FINANCIAL AND NON-FINANCIAL MARKET IN POLAND

2.1. FINANCIAL MARKET IN POLAND

2.1.1. Introduction

5. In Poland, the financial market is supervised by the Polish Financial Supervision Authority (KNF (PFSA)/PFSA). It was established pursuant to *the Act of 21 July 2006 on the financial market supervision* (Journal of Laws of 2017, item 196, as amended). From the first day of its activity, it took over the competences of the Securities and Exchange Commission, Insurance and Pension Fund Supervision Commission, whereas as of 1 January 2008, it also took over the tasks of the Banking Supervision Commission.

6. The Office of the Polish Financial Supervision Authority (UKNF (PFSA)) is a state legal person whose task is to provide services to the KNF (PFSA) (PFSA) and the Chair of the Polish Financial Supervision Authority.

7. The activities of the UKNF (PFSA) are supervised by the Prime Minister.

8. The governing bodies of the UKNF (PFSA) are:

- KNF (PFSA), which is responsible for the supervision of the financial market;
- The Chair of the KNF (PFSA) who manages the activities of the UKNF (PFSA) and represents the UKNF (PFSA) before third parties

9. The KNF (PFSA) exercises oversight of the banking sector, the capital, insurance, pension market, supervision over payment institutions and payment service offices, electronic money institutions and the savings and credit union sector.

10. In addition, tasks of the KNF (PFSA) comprise:

- undertaking measures to ensure the proper functioning of the financial market;
- undertaking measures aimed at the development of the financial market and its competitiveness;
- undertaking measures aimed at supporting the development of financial market innovation;
- undertaking educational and information actions in the scope of functioning of the financial market, its risks and entities functioning thereon in order to protect the justified interests of financial market participants,
- participation in drafting legal acts in the scope of financial market supervision;
- creating opportunities for amicable and conciliatory settlement of disputes between financial market participants, in particular disputes arising from contractual relations between entities subject to KNF (PFSA) supervision and recipients of services provided by these entities;
- performing other tasks as specified by laws.

11. The objective of financial market supervision is to ensure proper functioning of this market, its stability, security and transparency, confidence in the financial market, as well as to guarantee the protection of interests of this market participants

12. The KNF (PFSA) exercises the supervision in the following scope:

- banking supervision, exercised in accordance with the provisions of: *the Act of 29 August 1997. - Banking Law* (Journal of Laws of 2018, item 2187, as amended), *the Act of 29 August 1997 on National Bank of Poland* (Journal of Laws of 2017, item 1373, as amended), *the Act of 7 December 2000 on the functioning of cooperative banks, their association and associating banks* (Journal of Laws of 2018 item 613 as amended) and *Regulation of the European Parliament and of the Council (EU) no 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms amending Regulation (EU) No 648/2012* (OJ L 176, 27.06.2013, p. 1, as amended);
- pension supervision, exercised in accordance with the provisions of: *the Act of 28 August 1997 on the organisation and functioning of pension funds* (Journal of Laws of 2018, item 1906, as amended), *the Act of 20 April 2004 on employee pension schemes* (Journal of Laws of 2019, item 850), *the Act of 20 April 2004 on individual pension accounts and individual pension security accounts* (Journal of Laws of 2016, item 1776, as amended), *the Act of 22 May 2003 on insurance and pension supervision* (Journal of Laws of 2019, item 207), *the Act of 21 November 2008 on funded pensions* (Journal of Laws of 2018, item 926);
- insurance supervision, exercised in accordance with the provisions of: *the Act of 11 September 2015 on insurance and reinsurance activity* (Journal of Laws of 2019, item 381, as amended), *the Act of 15 December 2017 on insurance distribution* (Journal of Laws of 2018, item 2210, as amended), the *Act of 22 May 2003 on insurance and pension supervision* and the *Act of 7 July 2005 on insurance of agricultural crops and farm livestock* (Journal of Laws of 2019, item 477);
- supervision of the capital market, exercised in accordance with the provisions of: *the Act of 29 July 2005 on trading in financial instruments* (Journal of Laws of 2018 item 2286, as amended), *the Act of 29 July 2005 on public offering, conditions governing the introduction of financial instruments to organised trading and public companies* (Journal of Laws of 2019, item 623), *the Act of 27 May 2004 on investment funds and management of alternative investment funds* (Journal of Laws of 2018, item 1355, as amended), *the Act of 26 October 2000 on stock exchanges* (Journal of Laws of 2019, item 312, as amended), *the Act of 29 July 2005 on the capital market oversight* (Journal of Laws of 2018 item 1417 as amended), *Regulation of the European Parliament and of the Council (EU) No. 1227/2011 of 25 October 2011 on wholesale energy market integrity and transparency* (OJ L 326, 08.12.2011, p. 1)[1], the aforementioned Regulation No 575/2013, *Regulation of the European Parliament and of the Council (EU) No. 596/2014 of 16 April 2014 on market abuse (market abuse regulation) and*

[1] To the extent that it relates to wholesale energy products which are financial instruments and to which Article 2(1)(a) to (d) and (3) of *Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC* apply (OJ L 173 of 12.06.2014, p. 1, as amended).

repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (OJ L 173, 12.06.2014, p. 1 as amended), *Regulation of the European Parliament and of the Council (EU) No. 236/2012 of 14 March 2012 on short selling and certain aspects of credit default swaps* (OJ L 86, 24.03.2012, p. 1, as amended), *Regulation of the European Parliament and the Council no. 648/2012 of 4 July 2012 on OTC derivatives, central counterparties and trade repositories* (OJ L 201 of 27.07.2012, p. 1, as amended), *Commission Regulation (EU) No 1031/2010 of 12 November 2010 on the timing, administration and other aspects of auctioning of greenhouse gas emission allowances pursuant to Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowances trading within the Community* (OJ L 302, 18.11.2010, p. 1, as amended); R*egulation (EU) no. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012* (OJ L 257 of 28.08.2014, p. 1, as amended);

- supervision over payment institutions, small payment institutions, suppliers providing only the service of access to account information, payment service offices, electronic money institutions, branches of foreign electronic money institutions, exercised in accordance with the provisions of *the Act of 19 August 2011 on payment services* (Journal of Laws of 2019 item 659 as amended);
- supervision of credit rating agencies exercised in accordance with the provisions of *Regulation No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies* (OJ L 302, 17.11.2009, p. 1);
- supplementary supervision, exercised in accordance with the provisions of *the Act of 15 April 2005 on supplementary supervision over credit institutions, insurance companies, reinsurance companies and investment firms being part of a financial conglomerate* (Journal of Laws of 2016 item 1252 as amended);
- supervision over cooperative savings and credit unions and the National Cooperative Savings and Credit union, exercised in accordance with the provisions of *the Act of 5 November 2009 on cooperative savings and credit unions* (Journal of Laws of 2018 item 2386 as amended);
- supervision over mortgage loan intermediaries and their agents, exercised in accordance with the provisions of *the Act of 23 March 2017 on mortgage loan and supervision over mortgage loan intermediaries and agents* (Journal of Laws, item 819);
- supervision to the extent provided for by law: *Regulation (EU) No 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014* (OJ L 171, 29.06.2016, p. 1, as amended).

13. The supervision of the KNF (PFSA) does not cover the Social Insurance Institution, the Agricultural Social Insurance Fund, the Bank Guarantee Fund, the Insurance Guarantee Fund

and health insurance in the National Health Fund. They are subject to the oversight by the competent ministers.

Table no. 1 - Number of entities operating on the Polish financial market under the supervision of the KNF (PFSA) as of 31 December 2018[2]

Type of institution	Number of entities
banks operating in the form of joint stock companies (including 1 state bank, 2 banks associating cooperative banks)	32
cooperative banks	549
representative offices of credit institutions and foreign banks operating in Poland	12
savings and credit unions	31
domestic payment institutions	40
payment service offices	382
small payment institutions	10
mortgage loan brokers	852
mortgage loan broker agents	5861
brokerage houses	40
banks engaged in brokerage activities	9
investment firm agents	285
custodian banks	12
capital market infrastructure entities	4
investment funds[3]	878
investment fund companies (TFIs)	61
managers of alternative investment funds (AIFMs)	80
other entities providing services to investment funds or alternative investment funds[4]	204
commodity market infrastructure entities	2
commodity brokerage houses	1
energy companies keeping accounts or registers of exchange commodities	56
open pension funds	10
pension fund companies	10
employee pension funds	3
employee pension fund companies	3
depositories of pension funds	6
transfer agents of pension funds	6
voluntary pension funds	7
insurance companies of Class I (life insurance)	26
insurance and reinsurance companies of Class II (personal and non-life insurance)	34
insurance brokers	1374
reinsurance brokers	49

[2] Based on: Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2018, Warsaw 2019, pp. 11-12, available at: https://www.knf.gov.pl/publikacje_i_opracowania/sprawozdania

[3] The vast majority of funds are closed-end investment funds, i.e. 88.7% of all funds existing as of the end of 2018 (cf.: Report on the financial standing of investment fund companies in 2018, UKNF, Warsaw, May 2019, p. 6, available at: https://www.knf.gov.pl/?articleId=66075_id=18).

[4] Including entities entrusted with the performance of the duties of the TFI or AIF managers pursuant to the provisions of *the Act of 27 May 2004 on investment funds and alternative investment fund management* (Journal of Laws of 2018 item 1355 as amended).

14. Moreover, according to KNF (PFSA) data[5] - as of 31 December 2018, the following foreign entities have notified their activities in Poland in the form of branches:

- credit institutions (31);
- financial institutions (8);
- electronic money institutions (4);
- insurance companies (29);
- reinsurance companies (1);
- investment companies (15);
- management companies (1).

15. The KNF (PFSA) also keeps a register of the following types of entities (data as of 31 December 2018)[6]:

- insurance agents (31,427);
- persons performing agency activities (237,692);
- consumer credit intermediaries (27,917);
- lending institutions (421).

16. The President of the National Bank of Poland (NBP), as the body keeping the register of bureaux de change activities, performs the control of bureaux de change activities, in accordance with the provisions of *the Act of 27 July 2002. - Foreign Exchange Law* (Journal of Laws of 2019, item 160).

17. As of 31 December 2018, 2651 entrepreneurs possessing 5214 bureaux de change offices (of which 341 were suspended) were entered in the register of bureaux de change activities (in 2017, respectively - 2745 entrepreneurs owned 5240 currency exchange offices, including 289 suspended offices)[7].

2.1.2 Banking Sector

18. The legal framework of the Polish banking system is included in *the Act of 29 August 1997 - Banking law*. The above mentioned Act defines a bank as a legal entity established in accordance with the provisions of the statute and operating on the basis of licences authorising the performance of banking activities which expose funds entrusted to risk under any title of return. Banking activities which can only be performed by a bank pursuant to the *Act* of *29 August 1997 - Banking law*, include:

- accepting contributions in cash payable on demand or on the defined deadline and keeping accounts of such contributions;
- operating other bank accounts;

---

[5]Ibidem, p. 12
[6]Ibidem, p. 12
[7] Own report of the National Bank of Poland based on the data contained in the register of bureaux de change activities.

- granting credits;
- granting and confirming bank guarantees as well as opening and confirming letters of credit;
- issuing bank securities;
- performing banking monetary settlements;
- performance of other activities provided exclusively for the Bank in separate acts of law.

19. The following activities are also classified as banking activities, provided that they are performed by banks:

- granting cash loans;
- cheque and bill of exchange operations involving warrants;
- provision of payment services and issuance of electronic money;
- futures operations;
- purchase and disposal of cash receivables;
- storage of items and securities as well as making safe deposit boxes available;
- conducting the purchase and sales of foreign currency values;
- granting and confirming sureties;
- performing commissioned activities associated with issuance of securities;
- intermediation in money transfers and settlements in foreign exchange transactions;
- intermediation in concluding structured deposit agreements;
- consultancy in relation to structured deposits.

20. The activity of banks in Poland is also regulated by other legal acts, including the *Act of 29 August 1997 on the National Bank of Poland*, the *Act of 29 August 1997 on Debentures and mortgage banks* (Journal of Laws of 2016, item 1771), *the Act of 10 June 2016 on the Act on the Bank Guarantee Fund, the deposit guarantee scheme and compulsory resolution* (Journal of Laws of 2019 item 795 as amended) and *Regulation of the European Parliament and of the Council (EU) no 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms.*

21. Banks in Poland may operate and be created as state banks, banks in the form of joint stock companies (i.e. commercial banks) or cooperative banks.

22. Some of the above mentioned banks are authorised - on the basis of a license issued by the KNF (PFSA) - to conduct business activities pursuant to Article 70 (2) of *the Act of 29 July 2005 on trading in financial instruments* in the scope of*:*

1) accepting and transferring purchase or disposal orders of financial instruments;
2) executing orders referred to in subparagraph 1 on account of the person issuing the order;
3) purchase or disposal of financial instruments on own account;
4) management of portfolios comprising one or more financial instruments;

5) investment consulting;
6) offering financial instruments;
7) rendering services in the performance of concluded investment and service underwriting agreements or concluding and performing other agreements of similar nature if they involve financial instruments;
8) operating the ATS[8];
9) operating an OTF[9].

23. In accordance with the provisions of *the Act of 7 December 2000 on the functioning of cooperative banks, their association and associating banks*, in Poland banks associating cooperative banks operate.

24. The provisions of *the Act of 29 August 1997 - Banking law* also apply to the activities of credit institutions carried out on territory of Poland. Credit institution within the meaning of the aforementioned Act means an institution referred to in Article4(1)(1) of *Regulation (EU) No 575/2013 of the European Parliament and of the Council,* established in a Member State of the European Union other than the Republic of Poland. Pursuant to the aforementioned Article 4(1)(1)of *Regulation (EU) No 575/2013 of the European Parliament and of the Council*, a credit institution means an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.

25. Pursuant to Article 48i of *the Act of 29 August 1997 - Banking Law,*[10] a credit institution may operate in the territory of the Republic of Poland through a branch (other than a branch of a domestic bank[11] or a branch of a foreign bank[12]) or without opening a branch as a part of cross-border activity. It is undertaken in connection with the freedom to provide services within the European Economic Area (EEA), with the use of the principle of a single European passport. It is based on the fact that a credit institution which has received an authorisation/licence to conduct banking activity in one of the EEA Member States, shall not need to obtain additional authorisation/licence to conduct such activity in other EEA Member States. In the case of cross-border activity, a credit institution may only start cross-border activity "after the KNF (PFSA)has received a notification from the home country's competent supervision authorities determining the types of activities that the institution intends to carry out" (i.e. notification)[13].

26. At the end of 2018, the overwhelming majority of commercial banks and all branches of credit institutions were controlled by foreign investors, with investors from 18 countries, in particular Germany and Spain, holding controlling stakes in commercial banks. Domestic

---

[8] ATS - an alternative trading system, which is understood as a multilateral system, operated over-the-counter, matching bid and ask offers of financial instruments so that transactions are concluded within that system, in accordance with specified rules and in a manner other than discretionary.

[9] OTF - an organised trading facility, which is a understood as a multilateral system matching in a discretionary manner third party bid and ask offers for bonds, structured finance products, emission allowances, derivatives or wholesale energy products that must be executed by delivery, other than a regulated market or an ASO.

[10] Adequately to the rules indicated in Article 33 of *Directive 2013/36/EU on the conditions of admission of credit institutions to the activity and prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC* (OJ L 176, 27.06.2013, p. 338).

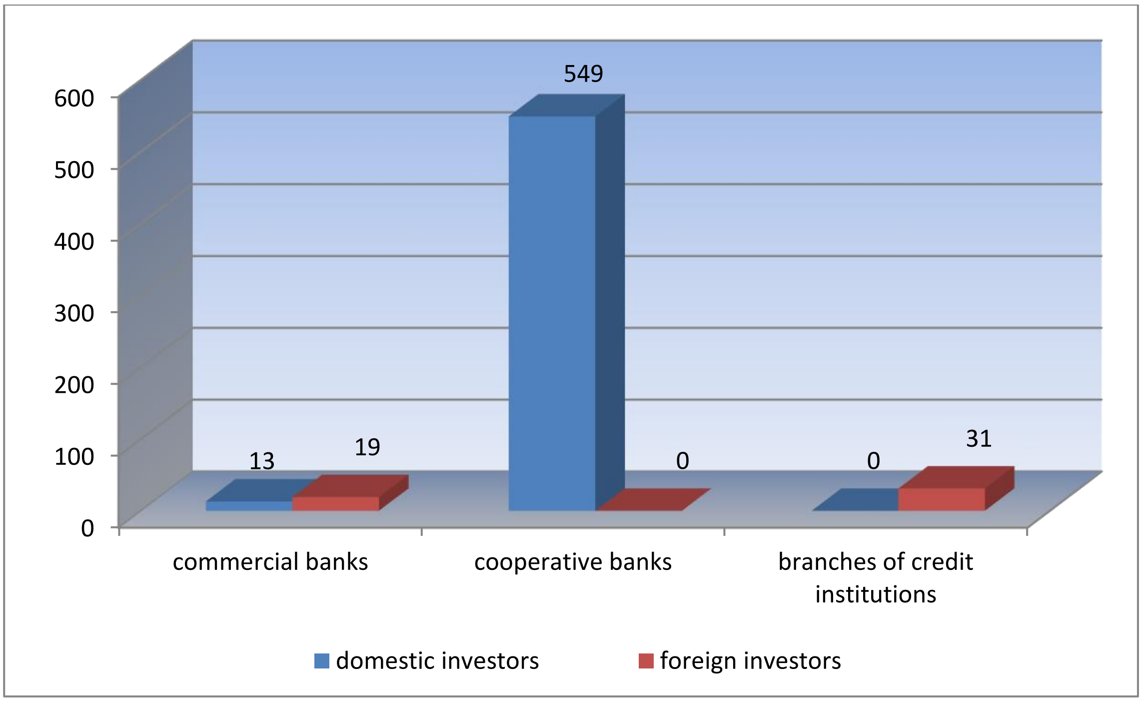
[11] i.e. a bank established in the territory of the Republic of Poland.

[12] i.e. a bank established in the territory of a non-EU Member State.

[13]Article 48ł of *the Act of 29 August 1997 Banking Law.*

investors controlled all cooperative banks as well as 13 commercial banks, including the State Treasury controlling 8 of them.[14]

Figure no. 1 - Number of banking sector institutions at the end of 2018 broken down into institutions controlled by domestic and foreign investors (according to the KNF (PFSA) data)



27. In connection with the acquisition of control over one of the commercial banks by the Polish capital in June 2017, the share of domestic investors in the assets of the sector became higher than the share of foreign investors, reaching the level of 54.5% at the end of 2017 (compared to 43.4% at the end of 2016). In 2018, the ownership structure of the sector did not change significantly, although the share of domestic investors in the assets of the banking sector decreased (to 53.6% at the end of 2018).

28. At the end of December 2018, the number of bank outlets amounted to 12,986 (in 2018 their number decreased by approx. 3.3%), while the employment in the banking sector amounted to 162,568 persons (i.e. 1.1% less than at the end of December 2017)[15]

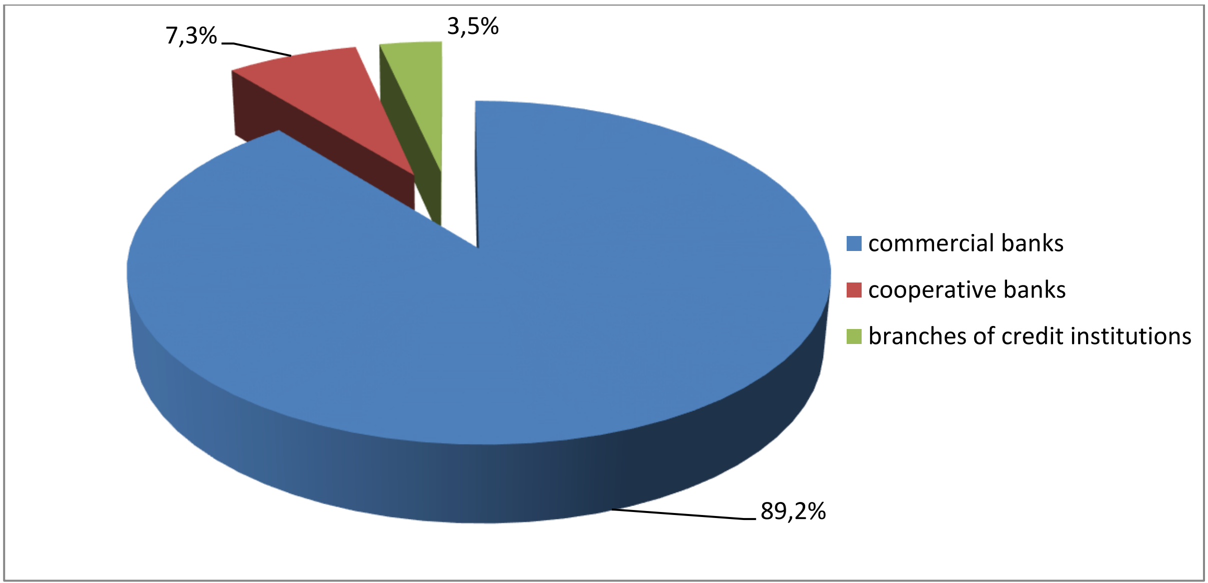
29. At the end of 2018, the concentration of the banking sector increased. The share of the 10 largest banks in the sector assets, loans to the non-financial sector and deposits from the non-financial sector amounted to 73.5%; 73.4% and 78.8%, respectively (70.1%, 69.3% and 74.6% at the end of 2017), which resulted from the purchase of bank assets by large banks.[16]

30. In 2018, the situation of the banking sector remained stable, which was fostered by the continued high economic growth rate, further improvement of labour market conditions as well as enhanced business and consumer sentiment. It is of significant importance for the country's

[14] Situation of the banking sector in 2018, UKNF (PFSA office), Warsaw 2019, p. 9, available at: https://www.knf.gov.pl/?articleId=65697_id=18.
[15] Ibidem, p. 8
[16] Ibidem, p. 9.

economy, especially in terms of the level of its assets. At the end of 2018, the value of financial system assets (without NBP) reached PLN 2.7 trillion, of which the banking Sector accounted for 75.1%.[17] The vast majority of the assets were managed by commercial banks.

Figure No. 2 - Share of individual categories of banking sector institutions in the total value of banking sector assets as of the end of 2018 (according to the KNF (PFSA) data)



31. At the end of 2018, 12 banks, accounting for 70.9% of the sector assets, were listed on the Warsaw Stock Exchange. Their total market value amounted to approximately PLN 578.9 billion, which represented 33.0% of the market value of all domestic companies listed on the WSE main market (trading in banks' shares accounted for 28.3% of the traded volume)[18]

2.1.3. Financial institutions, branches of financial institutions

32. A financial institution within the meaning of *the Act - Banking Law* shall mean a financial institution referred to in Article 4(1)(26) of *Regulation (EU) No 575/2013* of the *European Parliament and of the Council*. In accordance with this provision, a financial institution means an undertaking other than Annex I to a credit institution or an investment firm, the principal activity of which is to acquire holdings or to pursue one or more of the activities listed in points 2 to 12 and point 15 of Annex I to *Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on the conditions of admission of credit institutions to the activity and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC*. This terms includes financial holding companies, mixed financial holding companies, payment institutions within the meaning of *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC* (OJ L 319, 05.12.2007, p. 1) and asset management companies, but does not include insurance holding

[17] Situation of the banking sector in 2018, UKNF (PFSA), Warsaw 2019, p. 19, available at:https://www.knf.gov.pl/?articleId=65697&p_id=18

[18]Ibidem, p. 18

companies and mixed-activity insurance holding companies as defined respectively in Article 212(1)(f) and (g) of *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance* (OJ L 335, 17.12.2009, p. 1).

33. Thus, the definition of a financial institution within the meaning of the aforementioned Regulation 575/2013 and the *Act of 29 August 1997 - Banking Law* covers:

- undertakings whose principal activity is to perform one or more of the following activities: granting credit, leasing, payment services, issuing means of payment such as cheques, granting guarantees, trading in certain financial instruments (cheques, bills, certificates of deposit, foreign exchange, options and forward contracts, swaps, securities), participating in securities issues, advising on capital structure or industrial strategy and ownership transformations, money market intermediation, investment portfolio management and advice, safekeeping and administration of securities and issuing electronic money;
- payment institutions and holding companies of financial institutions (with the exception of insurance holding companies);
- credit granting institutions operating under the provisions of the *Act of 12 May 2011 on consumer credit* (Journal of Laws of 2018 item 993 as amended).

2.1.4. Payment institutions and electronic money institutions

34. *The Act of 19 August 2011 on payment services*[19] provides the basis for the functioning of a relatively new category of payment service providers and electronic money institutions. Article 2 of the aforementioned Act defines domestic electronic money institutions, hybrid electronic money institutions, branches of EU and foreign electronic money institutions, agents, settlement agents, domestic payment institutions, hybrid payment institutions, small payment institutions, hybrid small payment institutions, payment service offices, hybrid payment service offices, branches of EU payment institutions and suppliers providing only access to account information, operating in the territory of the Republic of Poland.

35. Depending on the scope of the permission granted by the KNF (PFSA), domestic payment institutions may provide all payment services from the catalogue contained in Article 3 of *the Act of 19 August 2011 on Payment Services*, i.e. the following services:

1) accepting cash payments and performing cash withdrawals from the payment account as well as any activities required to keep the account;

[19] This Act implements two EU directives: *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC* and *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.* This Act was significantly amended by *the Act of 10 May 2018 amending the Act on payment services and certain other Acts* (Journal of Laws of 2018, item 1075) published on 5 June 2018 which implemented *Directive of the European Parliament and the Council (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC* into the Polish legal system (OJ L 337, 23.12.2015, p. 35).

2) execution of payment transactions, including transfer of funds to a payment account with the user's provider or with another provider: by executing direct debit services, including single direct debits, with the use of a payment card or similar payment instrument, by executing credit transfer services, including standing orders;

3) performing payment transactions specified in subparagraph 2, debiting cash made available to the user on account of a loan and in the case of a payment institution or an electronic money institution - a loan referred to in Article 74(3) or Article 132j(3) of the aforementioned Act;

4) issuing payment instruments;

5) making acceptance of payment instruments possible and performing payment transactions initiated with a payer's payment instrument by the merchant or through the merchant, consisting in particular in the service of authorisation, sending payer's or merchant's payment orders to the payment instrument issuer or payment systems, with the aim of transferring due funds to the merchant, excluding activities comprising the clearing and settlement of such transactions within the payment system, within the meaning of the Act on settlement finality (acquiring);

6) providing the money remittance service;

7) providing the payment transaction initiation service;

8) providing the account information access service.

36. Payment service offices shall be authorised to provide only money remittance services. All categories of payment service providers are obliged to provide payment services in accordance with the provisions of the above mentioned *Act of 19 August 2011 on payment services*, concerning, inter alia, information obligations with respect to the provision of payment services, rights and obligations with respect to the provision and use of payment services.

37. The KNF (PFSA) keeps a register in which domestic payment institutions, small payment institutions, payment service offices, domestic electronic money institutions and branches of foreign electronic money institutions are entered.

38. Although both DPIs, SPIs and OPSs are entitled to provide payment services, there are significant differences between them, e.g. with respect to services acceptable for performance, territorial scope, legal form, licensing or registration obligations, capital requirements, transaction limits. Supervisory activities undertaken by the KNF (PFSA) with respect to the DPIs and the SPIs include, in particular, verification of standard statutory reporting, analysis of their financial results in terms of their compliance with the financial plans presented at the stage of licensing and registration proceedings, examination of their compliance with the applicable national and Community regulations.

39. The organisation associating national payment institutions is the Polish Organisation of Non-Bank Payment Institutions (PONIP).

40. As of the end of the third quarter of 2018, DPI own funds amounted to PLN 640.49 million, while taking into account statutory reductions[20] of PLN 204.86 million, DPI own funds, after reductions, amounted to PLN 434.98 million.[21] In the third quarter of 2018, DPIs executed 403.4 million payment transactions with a total value of PLN 34.9 billion. In the third quarter of 2018, the OPSs processed only 9.3 million money transfers with a total value of PLN 1.6 billion. Considering the fact that Krajowa Izba Rozliczeniowa S.A. (KIR S.A.) executed 449.51 million payment orders worth PLN 1,312.55 billion, payment transactions processed by DPIs in the third quarter of 2018 accounted for 89.75% of the orders executed by KIR S.A., whereas their value accounted for only 2.66% of the value of the transactions executed by KIR S.A. In connection with the foregoing, the importance of the sector of national payment institutions in the macroeconomic context is negligible.

41. In April 2019, the KNF (PFSA) issued the first licence for the electronic money institution.[22]

2.1.5. Brokerage activity

42. The basic legal act regulating the functioning of brokerage houses and offices on the territory of Poland is the *Act of 29 July 2005 on trading in financial instruments*

43. Within the meaning of the aforementioned Act, a brokerage house, a bank pursuing brokerage activities, a foreign investment firm[23] pursuing brokerage activities on the territory of the Republic of Poland and a foreign legal entity established on the territory of a country other than an EU Member State, pursuing brokerage activities on the territory of the Republic of Poland, are investment firms.

44. Running a brokerage business requires obtaining of the KNF (PFSA) license. Brokerage activities include, among others, accepting and forwarding orders to buy or sell financial instruments, buying or selling financial instruments on own account, managing portfolios that include one or more financial instruments, investment advice, offering financial instruments and providing services under the performance of investment and service underwriting agreements.

---

[20] Own shares or stocks held by a payment institution, measured at their balance sheet value, less impairment losses, any liabilities arising from the issue of preference shares, intangible assets measured at their balance sheet value, loss of the previous years, loss in the course of approval and net loss of the current period.

[21] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, p. 9, Warsaw 2019.

[22] https://www.knf.gov.pl/o_nas/komunikaty?articleId=65476_id=18date of reading 07.06.2019

[23] A foreign investment firm is a legal person or an organisational unit without legal personality established in the territory of another EU Member State, and if the regulations of a given country do not require the establishment of a registered office - with its head office in the territory of another EU Member State, or a natural person established in the territory of another EU Member State, pursuing brokerage activities in the territory of another EU Member State on the basis of a permit issued by a competent supervision authority as well as a foreign credit institution (i.e. a credit institution referred to in Article 4.1.1 of *Regulation (EU) No 575/2013*, conducting brokerage activities on the basis of an authorisation of a competent supervision authority in the territory of another EU Member State, or conducting brokerage activities on the basis of an authorisation of a competent supervision authority in the territory of another EU Member State, accounts on which securities admitted to trading on a foreign regulated market are registered).

45. In order to ensure due protection of investors' funds accumulated in brokerage houses, a compensation system has been established in Poland, managed by the National Depository for Securities (Krajowy Depozyt Papierów Wartościowych S.A.)

46. The organisation associating brokerage houses and offices in Poland is the Chamber of Brokerage Houses (IDM). The primary task of the IDM is to represent and protect the common interests of its members. The Chamber's obligations include in particular determination and codification of rules regarding fair trading in securities as well as customs adopted in trading.

47. As of 31 December 2018, the equity of brokerage houses amounted to PLN 1.79 billion (i.e. 2.19% more than at the end of 2017) and total assets - to PLN 6.61 billion (i.e. 2.54% less than at the end of 2017). The above mentioned entities generated a net profit in the amount of approx. PLN 164.74 million (i.e. 25.28% less than in 2017)[24]

48. At the end of 2018, brokerage houses operated 714,957 financial instrument accounts (i.e. 3.96% less than at the end of 2017). Customer assets worth over PLN 79.33 billion (i.e. 13.69% less than at the end of 2017) were deposited on these accounts. Customers' cash in the amount of approx. PLN 3.74 billion (an increase by 2.30% as compared to 2017) was deposited on cash accounts intended for their servicing.

49. In 2018, 15 brokerage houses carried out activities consisting in customer asset management (as of 31 December 2018, these entities managed customers' assets worth approximately PLN 6.62 billion).

50. In the brokerage house sector, the main business lines of the above mentioned entities are:

- raising funds for the benefit of issuers, in particular by offering their shares, bonds or investment certificates;
- accepting and forwarding client orders, in particular with respect to instruments listed on the Warsaw Stock Exchange (Giełda Papierów Wartościowych w Warszawie S.A. - WSE);
- management of clients' assets on request.

51. In addition, brokerage houses also provide other services related to the functioning of the broadly understood capital market and entities operating on it. Among such services one can mention e.g. activity in the form of an animator, service of calls and *de-listing of* companies, investment advisory services.

52. Apart from brokerage houses, some banks also operate as brokers. As of 31 December 2018, brokerage houses operated 1,113,066 accounts of customers' financial instruments (i.e. 6.65% less than at the end of 2017), on which financial instruments worth approximately PLN 185.83 billion were held (i.e. 8.82% less than at the end of 2017). Cash in the amount of approx. PLN 3.92 billion was deposited on cash accounts intended for service of financial instrument accounts (i.e. 0.92% more than at the end of 2017). While performing portfolio management services involving one or more financial instruments, brokerage houses managed customer assets worth approximately PLN 820.39 million (a decline by 33.53% compared to 2017).

[24] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, p. 11, Warsaw 2019.

53. At the end of 2018, custodian banks maintained 45,988 securities accounts (i.e. 13.12% more than at the end of 2017) where assets worth approximately PLN 959.95 billion were recorded (i.e. 7.09% more than at the end of 2017).

54. A commodity brokerage house is defined in Article 2(8) of *the Act of 26 October 2000 on commodity exchanges* as a joint-stock company or a limited liability company established on the territory of the Republic of Poland, pursuing brokerage activities in the scope of trading in exchange commodities. This type of activity covers the performance of activities consisting in:

- purchase or sale of exchange commodities on behalf of another person pursuant to the principles set forth in Article 38b of the aforementioned Act, including the settlement of the customers' transactions;
- keeping accounts or registers of exchange commodities, except for the commodities referred to in Article 2 (2)(a) of the aforementioned Act;
- advisory services in the scope of exchange trading.

55. Unless the Act provides otherwise, the Commodity Trading activities conducted on the Commodity Exchange may be conducted only by a commodity brokerage house.

56. According to the last audited financial statements (for 2017), the only brokerage house licensed by the KNF (PFSA) generated a profit of approximately PLN 511.59 thousand, its equity amounted to approximately PLN 7.94 million and total assets to approximately PLN 74.48 million.

57. The trading companies referred to in Article 50a of the aforementioned *Act*, i.e. trading companies other than commodity brokerage houses, may pursue brokerage activities consisting in the purchase or sale of exchange commodities for the account of a third party, including the settlement of customers' transactions and providing advice in the scope of exchange trading in exchange commodities. They are not subject to the requirement of obtaining a KNF (PFSA) license, therefore the aforementioned authority does not supervise their activity on commodity exchanges.

2.1.6. Investment funds

58. The investment fund sector comprises mainly investment fund companies managing open-end investment funds (FIO), specialist open investment funds (SFIO) and closed-end investment funds (FIZ).

59. The principles of establishing and operation of investment funds established on the territory of the Republic of Poland are defined in *the Act of 27 May 2004 on investment funds and alternative investment fund management*.

60. In accordance with the provisions of Article 3(1) of the aforementioned Act, an investment fund is a legal person acting exclusively in the scope of investing funds collected by means of public, and in certain cases defined in the Act, also non-public, offering of the purchase of participation units or investment certificates, in securities, financial market instruments and other property rights specified in the Act. An investment fund company acts as the governing body of the investment fund.

61. The investment fund may be established as: a FIO, a SFIO or a FIZ. Investment funds operating in Poland and fulfilling the requirements of the UCITS[25] Directive (i.e. funds harmonised with the Community law) are exclusively open-end investment funds. Other investment funds, i.e. closed-end investment funds and specialist open-end investment funds do not meet the requirements of the UCITS Directive, regardless the fact that their rules of operation are regulated by *the Act* of *27 May 2004 on investment funds*. Pursuant to Article 3(4) of the aforementioned Act, those funds are regarded as alternative investment funds (AIFs).

62. The operational security of investment funds, including the protection of rights of participants in investment funds, is based on several statutory pillars, namely: supervision by the Authority, separation of investment fund assets from those of the management company (investment fund companies) and subjecting the company to specific capital requirements, introduction of investment limits for particular types of investment funds, imposition of obligations on investment funds to provide fund participants and potential investors with specific information about the fund activities and financial standing.

63. The Chamber of Fund and Asset Management (IZFiA) is an organization which associates, on a voluntary basis, investment fund companies in Poland. The main objectives of the Chamber are to represent the environment of investment fund companies, support the development of investment fund companies in Poland, disseminate knowledge about investment funds, develop and improve the professional ethics of specialists related to the management of investment funds.

64. According to KNF (PFSA) data, as of 31 March 2018, 62 investment fund companies managing the total of 899 investment funds held a license of the Polish Financial Supervision Authority, i.e.: 44 FIOs, 55 SFIOs and 800 FIZs (including 29 public closed-end investment funds).

65. Table 2 below contains the information concerning the value of assets and net assets broken down by the type of fund as of 31 December 2017 and 31 March 2018.

Table no. 2 - Value of assets and net assets (in PLN million) broken down by types of funds

Description	**status as of 31 December 2017**	**status as of 31 March 2018**
Total value of assets	**314,068.21**	**330,965.48**
including FIO	*104,087.58*	*106,938.90*
including SFIO	*48,341.22*	*55,760.45*
including FIO	*161,639.42*	*168,266.13*
- public funds	*3,072.31*	*2,768.65*
Total value of net assets	**295,624.27**	**312,840.12**
including FIO	*96,653.51*	*98,549.72*
including SFIO	*235.43*	*318.48*
including FIO	*151,735.32*	*159,971.91*
- public funds	*2,649.98*	*2,546.73*

66. Due to the lack of completion of the process of submitting quarterly reports of investment funds by investment fund companies and supervisory verification of the information received,

[25] *Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)* (OJ L 302, 17.11.2009, p. 32).

the data concerning the value of assets and the value of net assets as of 31 March 2018 serve for reference only.

67. It should be stressed that the number and nature of participants in the fund largely depend on the type of fund. According to the data available in the KNF (PFSA) as of 31 March 2018, the total number of records related to the participation in the FIO or the SFIO was approximately 6.3 million, while this number should not be identified with the number of participants in the fund. It only shows an indicative number of investors investing their assets in such funds. On the other hand, with respect to the FIZ, it should be indicated that the number of its participants as of 30 June 2017 amounted to approximately 39 thousand whereas the value of assets of such funds accounted for approximately half of all types of funds.

68. The foregoing is determined by the type of investment policy pursued by a given type of fund. In the case of FIO and SFIO, it can be concluded that these funds invest mainly in assets listed on a regulated market. On the other hand, the investment policy pursued by the FIZ is much more flexible. They largely concentrate their assets on OTC investments. Hence, investments in certificates issued by the FIZ are much less liquid investments than the participation units issued by the FIO and the SFIO. Therefore, the FIZs attract investors with a higher level of acceptance for investment risk, but also with much higher resources.

69. Moreover, it should also be pointed out that foreign fund participation titles may be sold on the territory of Poland. As of 31 December 2017, 58 foreign funds were entered into the register of foreign funds and funds referred to in Article 262 of *the Act of 27 May 2004 on investment funds and management of alternative investment funds* which dispose of the participation titles on the territory of the Republic of Poland. The total value of participation titles of foreign funds sold on the territory of the Republic of Poland amounted to PLN 5.63 billion, which constituted 1.87% of the share of net assets of foreign funds in the total net assets of Polish and foreign funds.

70. Investment fund companies or investment funds may subcontract the performance of their activities to other entities, i.e.:

- transfer agents (keeping records of participants in investment funds);
- entities holding a KNF (PFSA) license to manage securitised receivables of the securitisation fund;
- distributors - entities other than entities pursuing brokerage activities;
- entities managing the investment portfolio of a fund or its part;
- entities managing the investment fund risk.

71. Since 4 June 2016, alternative investment company (AIC) managers have constituted a new group of investment fund sector entities.

72. Pursuant to Article 8a(1) of *the Act of 27 May 2004 on investment funds and alternative investment fund management*, the AIC is an alternative investment fund other than the fund referred to in Article 3(4)(2) of this Act, i.e. other than specialised open-end and closed-end investment funds created and operating under the Act. Therefore, the AIC is not an investment fund within the meaning of the Act.

73. It should be emphasised that the aforementioned Act defines an alternative investment fund (AIF) as an institution of common investment whose subject of activity, including within a separated sub-fund, is to collect assets from many investors in order to invest them in the interest of those investors in accordance with the specific investment policy, which is not a UCITS fund at the same time, i.e.: a fund acting in accordance with the EU law regulating the rules of collective investment in securities.

74. Pursuant to Article 8a(2) of the aforementioned Act, the AIC may operate in the form of a capital company, including a European company as well as a limited partnership or a limited joint-stock partnership, in which the only general partner is a capital company, including a European company.

75. Following the statutory definition of AIF, Article 8a(3) of that Law provides that the sole subject-matter of the AIC activity, subject to the exceptions laid down in the Act, is to collect assets from a large number of investors in order to invest them in the interests of those investors in accordance with a specific investment policy. The management of an alternative investment company, in accordance with Article 8b(1) of the aforementioned Act, comprises at least the management of the investment portfolio of that company and the risk and is exercised by the AIC manager.

76. Pursuant to Article 8b(2) of the aforementioned Act, the AIC may only be managed by a capital company being an AIC referred to in Article 8a(2)(1) of the aforementioned Act - operating as an internal AIC manager and a capital company that is a general partner of the AIC referred to in Article 8a(2)(2) of the Act - operating as an external AIC manager. Pursuant to Article 70e(1) of the aforementioned Act, the subject-matter of the AIC manager activity may be exclusively the management of the AIC, including introduction of the company to trading and the management of the EU AIF, including introduction of those AIFs to trading. An external manager of the AIC may manage more than one alternative investment company operating in the form set out in Article 8a(2)(2) of the aforementioned Act or more than one EU AIF, while an internal AIC manager of AIC may manage only that AIC company (self-management).

77. The performance of the activities of an AIC manager, both externally and internally, is regulated by the Act referred to above and, depending on the value of assets included in AIC investment portfolios which the particular AIC manager intends to manage or manages, requires either the license of the Polish Financial Supervision Authority pursuant to Article 70a et seq. of the aforementioned Act or the entry in the register of AIC managers kept by the Commission pursuant to Article 70zb et seq. of the Act.

2.1.7. Pension funds

78. The pension funds sector is a part of the pension scheme where assets of members are accumulated for future pension benefits.

79. The rules for establishing and operation of pension funds are laid down in *the Act of 28 August 1997 on the organisation and operation of pension funds.*

80. At present, the pension fund sector is dominated by Pension Fund Companies (PTEs) which manage Open Pension Funds (OFEs) and accumulate approximately 99% of the assets of all pension funds. Other funds operating on the market include Voluntary Pension Funds (DFE) and Employee Pension Funds (PFE) managed by Employee Pension Fund Companies (PrTE). Unlike the PFE and the DFE, which are fully voluntary in nature, in the past the OFEs were

compulsory for all pensioners within the meaning of the social security legislation. Currently, insured persons may only declare their willingness to transfer a part of their pension contribution. Irrespective of this declaration, OFE members cannot freely dispose of the accumulated funds which remain in the OFE and are gradually transferred from it to the Social Insurance Institution (ZUS) 10 years before reaching the retirement age based on the so-called safety slider.

81. At the end of 2018 Q1, 16 million participants in 11 OFEs held the total of PLN 165.7 billion of accumulated assets. For comparison, the DFEs and PFEs accumulated the total of PLN 2.1 billion of assets. Due to their mandatory status until 2014 and their current partially mandatory nature, the OFEs are subject to detailed regulations and supervision, especially in the area of investment activity. The catalogue of deposits available for the OFEs has been defined by the legislator with a view to the safety of funds entrusted whereas additional risk protection tools include investment limits and detailed information obligations, on which the indirect supervision exercised by the UKNF (PFSA office) is based. As part of their duties, the OFEs report daily, among others, the status of their investment portfolio with the accuracy as to the instrument, a set of transactions executed on instruments and other financial and operational data necessary to assess the compliance of pension fund activities with the provisions of law and the statutes as well as the interests of their members.

2.1.8. Cooperative Savings and Credit Unions

82. The activity of cooperative savings and credit unions is regulated by *the Act of 5 November 2009 on cooperative savings and credit unions*, whereas the provisions of *the Act of 16 September 1982 - Cooperative law* shall apply to matters other than regulated by the aforementioned Act .

83. The credit unions are cooperative entities whose objective is to collect cash only from its members, grant loans and credits to them, carry out financial settlements on their request and act as an intermediary in concluding insurance agreements. Members of the credit union may include:

- natural persons bound by professional or organisational links, in particular workers employed in one or more establishments and persons belonging to the same social or professional organisation;
- non-governmental organisations within the meaning of Article 3(2) of *the Act of 24 April 2003 on public benefit activity and volunteering* (Journal of Laws 2019, item 688) operating among credit union members;
- organisational units of churches and religious associations with legal personality;
- cooperatives;
- trade unions;
- housing cooperatives.

84. The activity of the credit unions is subject to supervision exercised by the KNF (PFSA) (PFSA). The scope and principles of this supervision are laid down in *the Act of 21 July 2006 on financial market supervision* and the *Act of 5 November 2009 on cooperative savings and credit unions*.

85. Situation of individual credit unions is diversified. There are savings and credit unions that operate safely as well as those in a difficult financial situation which need deep restructuring. At the end of 2018 Q3, 22 cash registers were subject to resolution proceedings (3 credit unions implemented programs approved by the KNF (PFSA)).[26]

86. According to preliminary data presented in the report on the activity of the KNF (PFSA) and the UKNF (PFSA office) in 2018, the assets of credit unions at the end of 2018 Q4 amounted to over PLN 9.6 billion. In 2018, they recorded a net loss of PLN 2.7 billion, mainly due to one of the credit unions, in relation to which the proceedings on its acquisition by a domestic bank were pending. Excluding the data on the activity of the credit union mentioned above, the credit union sector would generate a net profit of PLN 30.75 million. As of 31 December 2018, own funds of the credit unions reached the level of PLN 387.18 million (calculations compliant with the *Act on cooperative savings and credit unions of 5 November 2009*)[27]

2.1.9. Insurers

87. The legal basis for the performance of activities in the field of personal insurance and property insurance, reinsurance activity, as well as actuarial profession, insurance supervision, supervision over insurance and reinsurance companies in groups, organisation and operation of insurance business self-government is the *Act of 11 September 2015 on insurance and reinsurance activity*.

88. Pursuant to the aforementioned Act, insurance activity is understood as performing insurance activities related to offering and granting cover against the risk of occurrence of consequences of random events. On the other hand, reinsurance activity means performing activities related to accepting risks ceded by an insurance company or by a reinsurance company and further ceding of accepted risks.

89. The insurance activity may be carried on by an insurance undertaking only in the form of a joint stock company or a mutual insurance association or a European company as defined in *Council Regulation (EC) No 2157/2001 of 8 October 2001 on the Statute for a European company (SE)*[28]. The Act divided insurance according to classes, groups and types of risks. Class I is life insurance, while Class II is other personal and property insurance. An insurance undertaking may not simultaneously carry on activities in Classes I and II.

90. The reinsurance activity may be carried on by a reinsurance undertaking only in the form of a joint stock company, a mutual reinsurance association or a European company as defined in *Council Regulation (EC) No 2157/2001 of 8 October 2001 on the Statute for a European company (SE)*.

91. The performance of insurance or reinsurance activities requires obtaining a license from the KNF (PFSA).

[26] Information on the situation of cooperative savings and credit unions in 2018 Q3, Department of Credit Unions and Payment Institutions, UKNF (PFSA office), Warsaw, January 2019, p. 4, available at: https://www.knf.gov.pl/?articleId=64620_id=18.

[27] Ibidem, p. 15

[28] OJ L 294, 10.11.2001, p. 1.

92. The Polish Chamber of Insurance (PIU) is an institution established to represent domestic insurance companies, reinsurance companies and foreign insurance companies operating in the territory of the Republic of Poland. The PIU operates under the aforementioned *Act of 11 September 2015 on insurance and reinsurance activity*.

93. According to KNF (PFSA) data, at the end of March 2018, 21 companies had a majority share of the domestic capital (over 50%).

94. At the end of 2018 Q1, the value of assets of insurance companies reached the level of PLN 196.92 billion, where assets of life insurance companies accounted for 52.2% of this value. In that period, the net financial result of these entities amounted to PLN 1.06 billion, of which 44.3% was attributable to life insurance companies. It should be noted that the total of 17 life insurance companies (i.e. 27.9% of all insurance companies) reported a net financial loss.

95. Moreover, according to the KNF (PFSA) data as of 19 July 2018 - branches of insurance companies of EU member states and member states of the European Free Trade Agreement - parties to the agreement on the European Economic Area pursued their activity in the territory of Poland: 6 - in the scope of life insurance and 24 - in the scope of other insurance.

96. The scope of insurance activity also includes insurance intermediation. This activity consists in the performance of actual or legal activities relating to the conclusion or performance of insurance agreements by an intermediary against the remuneration. Insurance intermediation shall be performed exclusively by insurance agents or insurance brokers. Insurance intermediation in the scope of reinsurance shall be performed exclusively by insurance brokers holding the authorisation to perform reinsurance brokerage activities (reinsurance brokers).

97. The rules of conducting business activity in the scope of insurance intermediation are specified in *the Act of 22 May 2003 on insurance intermediation*.

98. Pursuant to Article 7 of the aforementioned *Act on insurance intermediation* , an insurance agent is an entrepreneur who has signed an agency agreement with an insurance company and is entered into the register of insurance agents (RAU) kept by the KNF (PFSA).

99. The environment of insurance intermediaries is associated the Polish Chamber of Insurance and Financial Intermediaries.

2.1.10. Companies operating a regulated market

100. Pursuant to Article 14 of *the Act of 29 July 2005 on trading in financial instruments*, the term "regulated market" shall mean "a permanently operating multilateral trading system for financial instruments admitted to trading in this system, providing investors with universal and equal access to market information at the same time when matching purchase and sale offers for financial instruments and equal conditions for the purchase and sale of such instruments, organised and subject to supervision by a competent authority on the principles specified in the provisions of the Act as well as recognised by a Member State as meeting these conditions and designated by the European Commission as a regulated market".

101. Pursuant to Article 21(1)-(2) of the aforementioned Act, the regulated market may be operated only by a joint-stock company. The subject-matter of its activity may be exclusively the operation of a regulated market, the ATS, the auction platform, the OTF, pursuing activity consisting in the provision of services in the scope of the provision of information on transactions or running other activities related to the organisation of trading in financial

instruments and activities related to such trading, subject to subparagraphs 3 and 3a of the aforementioned Act.

102. The functioning of the regulated market is supported by capital market infrastructure entities, including the WSE and BondSpot S.A. besides the National Depository of Securities (KDPW S.A.) and KDPW_CCP.

103. The core business of the WSE is the operation of a regulated market which operates on the basis of the Exchange Rules (amendments thereto are approved by the KNF (PFSA) and the Specific Exchange Trading Rules. The main subject of the Exchange trade focuses on securities: shares, bonds, pre-emptive rights, rights to shares, investment certificates and derivatives: futures contracts, options, index participation units[29]

104. Apart from the regulated market, the WSE also operates an organised market of financial instruments in the formula of an alternative trading system, i.e. NewConnect. It is intended primarily for young companies with a relatively limited anticipated capitalisation. Compared to the regulated market, it is distinguished by simplified formalities related to the introduction of financial instruments to trading as well as relatively lower début costs and less stringent disclosure obligations imposed on issuers[30].

105. Trading on the regulated market is also conducted by BondSpot S.A., supervised by the KNF (PFSA). It is mainly involved in trading in treasury, corporate and cooperative bonds and other debt securities. BondSpot SA also arranges trading in debt instruments within the alternative trading system (dematerialised bonds, mortgage bonds, covered bonds and other debt financial instruments incorporating property rights corresponding to rights arising from incurring a debt may be traded). In addition, it operates the second alternative trading system called *Treasury BondSpot Poland*.[31]

106. A company managing a regulated market may also operate an auction platform pursuant to the provisions of the *Act on trading in financial instruments* and *Commission Regulation (EU) No 1031/2010 of 12 November 2010 on the timing, administration and other aspects of auctioning of greenhouse gas emission allowances pursuant to Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowances trading within the Community*. (OJ L 302, 18.11.2010, p. 1), i.e. a platform to perform the functions referred to in Article 31(1) of that Regulation. In accordance with the provisions of the aforementioned Regulation, any Member State which does not participate in the joint action defined in Article 26(1) and (2) may appoint its own auction platform for the auctioning of its share of the volume of allowances covered by Chapters II and III of Directive 2003/87/EC to be auctioned pursuant to Article 31(1) of this Regulation.

107. On 20 December 2016, the KNF (PFSA) granted consent to one entity to operate the auction platform for CO_2 emission allowances.

---

[29]Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2018, p. 34, available at: https://www.knf.gov.pl/?articleId=65438&p_id=18.
[30]Ibidem, p. 35
[31]Ibidem, p. 36

2.1.11. National Depository of Securities (Krajowy Depozyt Papierów Wartościowych S.A.)

108. National Depository of Securities (KDPW S.A.) operates a central depository of securities and settlement of transactions in dematerialised securities. Moreover, the basic tasks of KDPW S.A. also include:

- supervision over the compliance of the size of the issue with the number of securities traded;
- handling corporate events;
- the fulfilment of issuers' obligations as well as the operation of a mandatory compensation scheme.

109. KDPW S.A. also operates a trade repository that collects and maintains data on OTC derivative transactions in a centralised manner.

110. The Polish Central Securities Depository was established in 1991 as one of the divisions of the Warsaw Stock Exchange (WSE). On 7 November 1994, this division was separated from the WSE and since then KDPW S.A. has been operating as an autonomous, independent joint-stock company with 1/3 of its shares held by the State Treasury, 1/3 by the WSE and 1/3 by the NBP.

111. KDPW S.A. holds 100% of shares in KDPW_CCP S.A., which is a clearing house. Since 8 April 2014, KDPW_CCP S.A. has been operating as a CCP pursuant to Article 14 in conjunction with Article 17 of *Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories* (OJ L 201, 27.07.2012, p. 1).[32]

112. KDPW_CCP S.A. clears transactions concluded in organised trading and in alternative trading venues as well as derivative OTC transactions and *repo* transactions. The said company organises a system for securing the liquidity of settlements accepted for the clearing of transactions[33]

2.1.12. Entities pursuing bureaux de change activity

113. Bureaux de change activity, as defined in *the Act of 27 July 2002 - Foreign exchange law* (Journal of Laws of 2019, item 160) is a regulated business activity consisting in the purchase and sale of currency exchange values and intermediation in their purchase and sale. The foreign exchange values traded in the framework of bureaux de change activity include foreign currencies, foreign exchange gold and foreign exchange platinum. Bureaux de change activity, as a regulated activity within the meaning of the provisions of the *Act of 6 March 2018 - Entrepreneur Law* (Journal of Laws, item 646, as amended), requires registration in the register of bureaux de change activity. The authority keeping the register is the President of the National Bank of Poland.

[32]In accordance with Article 2(1) of Regulation 648/2012, CCP means “a legal person operating between counterparties of contracts traded on at least one financial market, becoming a purchaser for each seller and a seller for each purchaser”.

[33]Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2018, p. 38, available at: https://www.knf.gov.pl/?articleId=65438&p_id=18.

114. In accordance with the data stemming from the register of bureaux de change activity, as of 31 December 2018, 2651 entrepreneurs pursuing bureaux de change activity in 4873 bureaux de change offices in Poland were entered into the register of bureaux de change activity (in 2017 - 2745 entrepreneurs pursuing bureaux de change activity in 4951 bureaux de change offices).

115. Bureaux de change activity may be carried out by natural persons who have not been legally convicted of a fiscal offence or an offence committed for the purpose of obtaining financial or personal gain as well as by legal persons and companies without legal personality whose no member of the authorities or partner, respectively, has been convicted of such an offence.

116. Activities directly related to the performance of bureaux de change activity may be carried out only by persons (cashiers) who have not been convicted of the above-mentioned offences and have a professional preparation to perform these activities. Completion of a course covering legal and practical issues related to pursuing bureaux de change activity (documented by a certificate) or working in a bank for at least one year in a position directly related to handling foreign exchange transactions (documented by a certificate of employment) and knowledge of the provisions of the Act regulating bureaux de change activity, confirmed by a submitted declaration, are considered as professional preparation.

2.1.13. Other entities providing the services of currency exchange or currency exchange intermediation

117. In addition to entrepreneurs pursuing bureaux de change activity, currency exchange services are also offered by entities that conduct currency exchange over the Internet and by entities that collect and match currency exchange orders from various customers and organise/enable such exchange between them. These entities operate on the basis of, inter alia, *the Act of 6 March 2018 - Entrepreneur Law*.

118. According to information available on the Internet, in 2017 over 50 online bureaux de change offices existed and about 35% of currency exchange transactions took place online[34] According to the information posted on the website [35]www.przeglad-finansowy.pl, it is possible to identify 34 websites of so-called online bureaux de change offices (also called e-cantors) on the Internet. They also include offices which belong to banks or entrepreneurs pursuing bureaux de change activity. In addition, the Internet offers 6 platforms for the exchange of foreign currency among users, also called social currency exchange platforms (i.e. based on the model of matching the purchase/sale offers of foreign currencies of individual users of the particular platform) as well as 3 platforms for group purchases of currency.

119. In the case of the latter type of platform, currencies are exchanged on the interbank market by collecting purchase/sale orders for the specific currency from multiple participants. Subsequently, the cumulative transaction is carried out on the foreign exchange market. This allows to reduce exchange costs.

[34] Poles exchange currencies on the Internet. Report - foreign currency exchange trends in the first half of 2017, Xchanger and Fintek.pl, 2017, p. 2, available at: https://fintek.pl/najnowszy-raport-kantorach-internetowych-polsce/.
[35] https://www.przeglad-finansowy.pl/p/internetowe-kantory-wymiana-walut-w.html, 18.02.2019.

2.2. NON-FINANCIAL MARKET

120. *Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering* (OJ L 166, 28.6.1991, p. 77) defines money laundering in the category of drug offence and imposed obligations on the financial sector only. However, the 2001 revision of the Directive already extended the scope both in terms of offences and professions as well as areas of activities covered by anti-money laundering and counter-terrorist financing legislation. Namely, it was proposed to extend the scope of criminal offences covered by the Directive to include a wide range of non-financial activities and professions susceptible to money laundering.

121. Many categories of actors offering various types of services and products that can be used for criminal purposes, including money laundering and financing of terrorism operate outside the financial market. The majority of them are the obligated institutions in accordance with the provisions of the *Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism*. In accordance with the above-mentioned Act, all these obligated institutions outside the financial sector have specific obligations, which must be unconditionally fulfilled in the manner defined in its provisions.

2.2.1. Gambling

122. In 2016- 2017, the functioning of the gambling market in Poland was regulated by *the Act of 19 November 2009 - gambling law (*Journal of Laws of 2019, item 847) and the implementing acts thereto. Pursuant to the Act, gambling games include games of chance, betting, card games and games on gaming machines.

1) Games of chance shall be games, including those arranged online, where the prize is either cash or a material prize and where the result depends primarily on chance. They include: number games, lotteries, telebingo, cylindrical games, dice games, cash bingo game, raffle bingo game, raffle lotteries, promotional lotteries, audiotele lotteries.

2) Mutual bets are bets on winnings in cash or in kind, consisting in guessing the results of sporting competition between people or animals, in which participants pay stakes, and the amount won depends on the total amount of paid stakes - lotteries and the occurrence of various events, including virtual events, in which participants pay stakes, and the amount won depends on the ratio of payment to win agreed between the host bet and the payer - bookmaking.

3) Games on gaming machines shall be games of chance that are played with the use of mechanical, electromechanical or electronic devices, including computer hardware and games corresponding to the rules of games on gaming machines arranged via Internet, where the prizes are either cash or in kind prizes and where the game contains an element of a lottery.

4) Card games include black jack, poker and baccarat, as long as they are played in order to win cash or in kind prizes.

123. The operation of activity in the scope of number games, cash lotteries, telebingo games on gaming machines outside the casino and the organisation of online gambling (with the exception of betting and promotional lotteries) is subject to the State monopoly.

124. Depending on the type of gambling in accordance with *the Act of 19 November 2009 - gambling law*, the organisation of gambling games requires a concession or a licence from the minister competent for public finance or a licence from the competent director of the Revenue Administration Regional Office or, alternatively, a notification of the competent director of the Revenue Administration Regional Office. Table 3 presents the number of entities operating in this area.

Table no 3 - Number of entities operating in the field of games of chance, betting, card games and games on gaming machines[36]

Item	**Number of entities**	
	2017 [37]	2018 *(preliminary data)*
Number games (monopoly)	1	1
Cash lotteries (monopoly)	1	1
Casinos	8	9
Game machine arcades	0	1
Betting	9	15
at ground points	8	10
via the Internet	7	14
Audiotele lotteries	18	15
Promotional lotteries	132	*No data*

125. As of the end of 2017, 49 casinos operated in Poland, 28 licences for arranging betting (including 2510 outlets accepting betting) and 7 licences for arranging betting via the Internet were effective.[38]

126. In Poland, a location limit for casinos in Poland is effective - no more than one casino per full 650,000 inhabitants of the province. The maximum number of gaming machines allowed in casinos was also introduced - up to 70.

127. The ban on playing poker between players in casinos is also effective outside the tournaments organised in these casinos.

128. Gambling game revenues reported by entities pursuing activities in the scope of gambling games in 2017 amounted to PLN 12.9 billion in total (in 2016 - PLN 10.6 billion).[39] The highest revenues were generated from number games and cash lotteries (PLN 4.6 billion and PLN 4.6 billion, respectively) as well as from casinos (PLN 4.8 billion and PLN 4.3 billion, respectively).

2.2.2. Post office operators

129. In accordance with Article 3(12) of *the Act of 23 November 2012 - Postal Law* (Journal of Laws of 2018, item 2188, as amended), the postal operator is an economic operator authorised to perform postal activity on the basis of an entry in the register of postal operators. The Postal Law also provides for the existence of a designated operator - a special type of postal operator

[36] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, Warsaw 2019, p.20.
[37] On the basis of: Information on the implementation of the Act - gambling law in 2017, Ministry of Finance, Warsaw 2018, p. 13, available at: https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/raporty/.
[38] Information on the implementation of the Act - gambling law in 2017, Ministry of Finance, Warsaw 2018, p. 10, available at: https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/raporty/.
[39] Ibidem, p. 15

obliged to provide postal services. Until 1 January 2016, the designated operator was Poczta Polska S.A. The register of postal operators is maintained by the President of the Office of Electronic Communications (hereinafter referred to as the UKE). Covering postal operators with the obligations of the Act was necessary to ensure the tightness of the system of counteracting money laundering and financing of terrorism since they provide, inter alia, postal money order services both in domestic and cross-border trade.

130. In 2017, the total volume of postal services decreased from 1.90 billion items to 1.87 billion items, which means a decrease by 1.6% y/y[40]

131. Poczta Polska S.A. (hereinafter referred to as "Poczta Polska"), as the designated operator, continued to play the most important role on the market in 2017 providing 1,564.8 million services in the domestic and foreign stream in 2017 (83.8% share in the total volume).[41]

132. In 2017, the number of postal operators decreased. As of the end of the year, there were 280 entities in the register of postal operators (in 2016 - 291), of which 143 were active in the provision of postal services (in 2016 - 156).[42]

133. Regulatory, control, mediation and inspiration activities within the postal and telecommunications market are performed by the President of the UKE. This authority is the central government administration authority. The scope of its competence is defined by the provisions of the Telecommunications Law and the Postal Law.

134. Pursuant to the decision of the UKE President of UKE, the operator designated to provide universal services in 2016 - 2025 is Poczta Polska. The designated operator shall be obliged to provide universal services across the territory of the country in a uniform manner in comparable conditions. In 2017, the subject-matter of postal activity of the designated operator included, in particular universal postal services in the domestic and cross-border trade: unregistered letters, registered letters (including registered letters, letters with declared value), consignments for the blind, postal parcels with the weight up to 20 kg (including with declared value) and M-bags, services included in the scope of universal services in the domestic and cross-border trade: letters (including unregistered, registered letters and letters with declared value) from bulk and other senders, courier services in domestic trade, courier services in cross-border trade, other postal services in domestic trade (among others: marketing consignments, advertisements, unaddressed printed matter, postal money orders, postal telegram, consignments with the weight over 10 kg and other), other postal services in cross-border trade (cross-border postal money orders and other).

135. In accordance with *the Act of 23 November 2012 - Postal law*, postal activity is a regulated activity within the meaning of the provisions of *the Act of 6 March 2018 - Entrepreneur Law* and requires an entry into the register of postal operators.

136. At the end of 2017, the total value of the Polish postal service market amounted to PLN 8.4 billion.

---

[40]Report on the situation of the postal sector in 2017, UKE, Warsaw, May 2018, p. 6, available at: https://bip.uke.gov.pl/download/gfx/bip/pl/defaultaktualnosci/23/16/1/raport_o_stanie_rynku_pocztowego_w_2017_roku.pdf.

[41]Ibidem, p. 7.

[42]Ibidem, p. 7.

137. In accordance with the current legal status, postal money orders are not included in the catalogue of universal services. The total volume of postal money orders in 2017 amounted to 42.5 million pieces[43]

138. The segment with the highest value on the Polish postal service market is the courier mail segment which has been increasing its value for the last few years at a rate of even a few hundred million PLN annually. In 2016, it covered 16.5% of the total volume of postal services on the market, making 47.2% of its value[44]

139. As of 31 December 2017, Poczta Polska had 7564 post offices.[45] On the other hand, alternative postal operators reported the total of 14,328 post offices.[46]

140. In 2017, the President of the UKE acquired control over 17 postal operators, including 7 entrepreneurs with respect to which premises existed that they conducted postal activity without the required entry in the Register of Postal Operators and the President of the UKE conducted inspections of Poczta Polska as the designated operator.[47]

2.2.3. Liberal legal professions

141. The liberal professions are regulated professions, i.e. they are described normatively in the detailed regulations. They have a service nature, defining the specific type of services, most often of non-material nature, with the specific relations between the liberal profession and the client. The purpose of activity of persons practising the liberal legal profession is the care for the safety of legal transactions. Liberal legal professions are professions of public trust, they have a regulated nature (special control both on the part of the legislator and individual corporations). Exercising of the liberal profession is independent and personal, of an intellectual nature. The liberal profession is associated with the possession of high skills and knowledge. Liberal professions are assigned to each individual corporation.

142. The concept of the liberal profession is not defined normatively but it is used in *the Commercial Companies Code* (ksh) in relation to a partner company. The ksh does not specify the meaning of the liberal profession concept but indicates the types of liberal professions that may be partners of the aforementioned company. In accordance with the ksh, liberal professions include, among others, legal or similar professions, including an attorney, a tax advisor, a notary, a legal advisor.

143. The attorney is a lawyer providing legal assistance under *the Act of 26 May 1982 - Law on attorneys' profession*, in particular consisting in providing legal advice, preparing legal opinions, drafting legal acts and appearing before courts and authorities.

144. The attorney is bound to keep secrecy of anything he/she learnt about in connection with providing legal assistance. The obligation to keep secrecy shall be unlimited in terms of time.

[43] Report on the situation of the postal sector in 2017, UKE, Warsaw, May 2018, p. 38, available at: https://bip.uke.gov.pl/download/gfx/bip/pl/defaultaktualnosci/23/16/1/raport_o_stanie_rynku_pocztowego_w_2017_roku.pdf.
[44] Ibidem, p. 22.
[45] Ibidem, p. 40.
[46] Report on the situation of the postal sector in 2017, UKE, Warsaw, May 2018, p. 43, available at: https://bip.uke.gov.pl/download/gfx/bip/pl/defaultaktualnosci/23/16/1/raport_o_stanie_rynku_pocztowego_w_2017_roku.pdf.
[47] Ibidem pp. 52-53.

The attorney may not be released from the obligation to keep professional secrecy with regard to facts of which he/she has become aware by providing legal assistance or by dealing with a case. The obligation to keep the professional secrecy shall not apply to information made available pursuant to the regulations on counteracting money laundering and financing of terrorism- to the extent defined under these provisions.

145. The bodies of the legal bar at central level include: National Bar Association, Supreme Bar Council, Higher Disciplinary Court, Disciplinary Ombudsman, Higher Audit Committee. At the regional level, bar associations exist that bring together attorneys and trainee attorneys. The bodies of the bar include: the Bar Assembly, the Regional Bar Council, the Disciplinary Court, the Audit Committee. The Supreme Bar Council, bar associations and bar teams shall have legal personality. The highest body of the self-government is the Supreme Bar Council, whereas in the region - the Regional Bar Council.

146. The right to practise the profession of an attorney is only granted to a person who has been entered in the list of attorneys by the Regional Bar Council. In accordance with the information contained in the National Register of Attorneys and Trainee Attorneys kept by the Supreme Bar Chamber, as of 18 March 2019, there were 18,571 active attorneys[48] and 107 foreign attorneys providing legal assistance[49]

147. In accordance with Article 1 §1-2 of *the Act - Notary Public Law of 19 February 1991* - (Journal of Laws of 2019, item 540 as amended), a notary public, within the scope of his/her powers, acts as a person of public trust, taking advantage of the protection conferred on civil servants whereas notarial activities performed by a notary public in compliance with the law take a form of an official document. The notary's task is to ensure the security and regularity of legal transactions (according to Article 80 § 2 of the aforementioned *Act* , a notary is obliged to take care of due protection of the rights and legitimate interests of parties and other persons for whom this activity may cause legal effects, while performing notarial activities).

148. According to the data of the Ministry of Justice, as of 31 December 2018, 3526 notaries[50] were appointed in Poland. On 2 April 2019, the Council of the Notariats of the European Union launched a new version of the European Census of Notaries. The platform is available in 23 languages and contains a list of approximately 40,000 notaries from the 22 EU Member States where the notaries public operate.

149. The professions of legal advisor and tax advisor are linked with the profession of the attorney. The basic difference between legal advisers and attorneys is the possibility to provide legal assistance in the employment relationship (available to legal advisers), until 1 July 2015 it was also the possibility to act as a defender in criminal proceedings, i.e. in criminal and fiscal penal cases (available to attorneys).

150. The existing classification into two corporations is considered artificial. For this reason, concepts are being put forward for merging legal advisers and attorneys within a single corporation. However, the classification into two corporations, has a practical and substantive basis: the legal adviser in an employment relationship should not be a defender in a criminal case since a concern arises regarding the independence of his/her decision in relation to his/her

---

48 http://rejestradwokatow.pl/adwokat/ewidencja, 18.03.2019
49 http://rejestradwokatow.pl/prawnikzagraniczny/ewidencja, 18.03.2019
50 http://sejm.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=B9ZJTY, date of reading 22 May 2019.

employer. The attorney is not a subject subordinate to his/her superiors, therefore no professional pressure is exerted on him/her.

151. The legal advisor is a lawyer providing legal assistance under the provisions of *the Act of 6 July 1982 on legal advisers*. The profession of a legal advisor is a profession of public trust and legal advice provided by the legal advisor consists in particular in providing legal advice and consultation, drafting legal opinions, drafting legal acts and appearing before authorities and courts as a proxy or a defender, including appearing before the Supreme Court, the Constitutional Tribunal, the Supreme Administrative Court, the Court of Justice of the European Union and the European Court of Human Rights. There are no restrictions concerning the entities to which a legal advisor may provide legal advice.

152. Legal advisers may practise in the office of a legal advisor, under a civil-law contract, in a civil partnership, general partnership, limited partnership, limited partnership and limited joint-stock partnership, and in the form of the employment contract.

153. Due to its nature, the profession of a legal advisor is most similar to the profession of an attorney. In the scope of rights, the only difference lies in the fact that legal advisers - unlike attorneys - may exercise their profession also in the employment relationship (however, in such circumstances, they may not act as defenders in cases concerning fiscal offences and crime, unless they relate to the employment relationship of the scientific and research and teaching staff).

154. A legal advisor is bound to keep secrecy of anything he/she learnt about in connection with providing legal assistance. The obligation to keep secrecy shall be unlimited in terms of time. The legal advisor may not be released from the obligation to keep professional secrecy with regard to facts of which he/she has become aware by providing legal assistance or by dealing with a case. The obligation to keep the professional secrecy shall not apply to information made available pursuant to the regulations on counteracting money laundering and financing of terrorism- to the extent defined under these provisions.

155. Each legal advisor and trainee is a member of the professional self-government and such membership is compulsory. The role of the self-government is to provide conditions for the performance of tasks of legal advisers specified in the Act, represent legal advisers and trainees and protect their professional interests. According to the list *Rejestrradcow.pl* maintained by the National Chamber of Legal Advisers, as of 12 November 2018 there were 45,696 legal advisers entered in the list of legal advisers (both exercising and not exercising their profession)[51]

156. Organisational units of the self-government of legal advisers, having legal personality include: the National Chamber of Legal Advisers and the District Chambers of Legal Advisers.

157. A tax advisor is a profession of public trust, exercised under *the Act of 5 July 1996 on tax advisory services*.

158. Tax advisory services include providing advice, opinions and explanations regarding tax obligations, preparing tax returns and tax declarations or providing assistance in this respect,

---

[51] According to the information contained in the search engine of legal advisers, made available by the National Chamber of Legal Advisers, as of 18 March 2019, there were 45,622 active legal advisers (http://kirp.pl/wyszukiwarka-radcow-prawnych/, 18.03.2019.).

representing clients in proceedings before tax authorities in all instances and before Administrative Courts, providing advice, opinions and explanations and conducting settlements other than taxes - such as public law receivables (e.g. Social insurance contributions and health insurance). They also include advisory services in the scope of international tax law, advice and representing clients in the scope of obligations arising from customs law, keeping tax books and other records for tax purposes and providing assistance in this area, advisory services in the scope of use of EU funds as public aid for entrepreneurs and other activities permitted under *the Act on tax advisory services*.

159. Professional performance of tax advisory services is subject to statutory protection, and their performance by unauthorised entities is prohibited and is subject to a fine. A tax advisor is obliged to conclude a professional civil liability insurance agreement.

160. A tax advisor must be highly qualified and his/her qualifications must be confirmed by a passed state examination.

161. A tax advisor is obliged to keep secret facts and information which he/she learnt in connection with his/her professional activity. These rules apply, accordingly, to persons employed by a tax advisor and entities referred to in Article 4(1) of *the Act on tax advisory services*, in the scope of performing tax advisory activities by these persons.

162. The National Chamber of Tax Advisers (KIDP) is a professional self-government of tax advisers entered in the list. It supervises the due performance of the tax advisor's profession. The membership of tax advisers to the above mentioned chamber is obligatory and arises upon being entered in the list.

163. The highest authority of the Chamber is the National Assembly of Tax Advisers (representatives of 16 Regional Branches of the Chamber elected during regional elections), convened once every 4 years. In the periods between the Assemblies, the activities of the self-government are managed by the National Council of Tax Advisers (consisting of 34 persons elected by the Assembly). The KIDP operates in 16 Regional Branches located in capital cities of the provinces.

164. Within the professional self-government the two-instance disciplinary judiciary operates.

165. According to information of 18 March 2019, 8929 persons were entered in the list of tax advisers.[52]

2.2.4. Bookkeeping services

166. Bookkeeping services, pursuant to Article 76a(1) of *the Accounting Act of 29 September 1994* (Journal of Laws of 2019, item 351), is a business activity within the meaning of the provisions of *the Act of 6 March 2018 - Entrepreneur law*, consisting in providing services in the field of keeping accounting books, determining and checking the status of assets and liabilities, valuation of assets and liabilities, determining the financial result, preparing financial statements and collecting and storing accounting evidence and other documentation.

167. Until 9 August 2014, activities involving the provision of bookkeeping services could have been performed only by authorised persons, i.e. persons holding a qualification certificate of the Minister of Finance or an accounting certificate of the Minister of Finance as well as

[52] https://krdp.pl/doradcy.php, 18.03.2019

auditors and tax advisers. Provisions of *the Act of 9 May 2014 on facilitating access to certain regulated professions* (Journal of Laws, item 768) introduced deregulation of this profession[53] Currently, any entrepreneur may undertake the activity consisting in the provision of bookkeeping services, provided that the bookkeeping activities are carried out by persons who:

- have full capacity to perform legal acts;
- have not been convicted by a final and binding court judgement of an offence against the reliability of documents, property, economic turnover, trading in money and securities, a fiscal offence and offences specified in Chapter 9 of *the Accounting Act* of *29 September 1994*.

168. An additional condition for conducting the activity consisting in bookkeeping services is the requirement that the entrepreneur, no later than on the day preceding the day of commencement of business activity, concludes a civil liability insurance agreement for damages caused in connection with the business activity in the field of bookkeeping services.

2.2.5. Foundations and associations

169. In accordance with the provisions of *the Act of 6 April 1984 on Foundations* (Journal of Laws of 2018, item 1491), the objectives of the foundation must be consistent with the fundamental interests of the Republic of Poland. In addition, they must be socially and/or economically useful. The definition of the goal is a constitutive element of each foundation. Clarifying this objective gives the foundation the specific individuality. This is done in the foundation act. It cannot be changed later. It can only be modified if a number of requirements are met. Foundations may pursue several objectives at the same time. Foundations are obligated institutions not upon the entry in the National Court Register but only to the extent they accept or make payments in cash of the total value equal to or exceeding the equivalent of EUR 10,000, regardless of whether the payment is performed as a single operation or as several operations which seem linked with each other.

170. A Foundation is a legal form of a non-governmental organisation in which the capital allocated for the specific purpose is an important element. In accordance with the provisions, the objective of the foundation must be socially or economically useful such as: health care, development of the economy and science, education and upbringing, culture and art, social care and welfare, environmental protection and care over monuments. The Foundation shall have legal personality. A foundation may be established by a natural or legal person (regardless of whether it has a social or profit-making purpose). Establishing a foundation requires a declaration before a notary public on the establishment of a foundation (possibly in a will), acceptance of the statute by the founders and submission of an application for registration of

[53] In 2019, the Ministry of Finance published a report on a nationwide survey on the assessment of the effects of deregulation (conducted from 20 August 2018 to 30 September 2018). In the summary of the survey it was indicated, among others, that "... in the last 4 years, the quality of services provided by accounting offices has decreased and although this may have been the effect of other factors, not only deregulation, it is an alarming phenomenon which requires undertaking appropriate measures. Moreover, no effective market certification mechanisms have been developed, since the certificates appearing on the market, licenses are not widely recognised and do not enjoy such trust as the accounting certificate issued by the Minister of Finance" (cf.: Report from a nationwide survey on the assessment of the effects of deregulation in bookkeeping services carried out in 2014, Ministry of Finance, March 2019, p. 58, available at: https://www.gov.pl/documents/1079560/1080340/20190408_raport_z_badania_ankietowego.pdf/2a52c700-5882-ad6f-2331-ac233ddd0a63).

the foundation to the National Court Register. Through registration, the foundation acquires legal personality.

171. There is no minimum initial capital in the regulations, but in practice it is assumed that a foundation not conducting business activity should have the initial capital at a minimum level of PLN 1,000 and a foundation conducting business activity - PLN 2,500 (however, the value of funds allocated for business activity cannot be lower than PLN 1,000).

172. The only obligatory body of the foundation is the Management Board. The scope of competence of individual foundation bodies and the method of making decisions must be defined in the statute. The Foundation may have employees both dealing with administrative matters and carrying out statutory activities. Employees may be founders, members of the authorities but also individuals from outside the foundation authorities.

173. Irrespective of whether the foundation has a public benefit status or not, it may carry out economic activity under the following conditions:

- the pursuit of economic activities must be provided for in the statute;
- assets in the amount of at least PLN 1,000 must be allocated for this activity;
- the foundation must be registered in the Register of Entrepreneurs maintained by the National Court Register;
- the economic activity must be ancillary to the core statutory activity.

174. The assets transferred to the foundation must be used for the implementation of statutory activities and it is not possible to return the initial capital to the founders. Unlike associations, the law does not require that all income from the economic activity of the foundation are allocated to its statutory activity.

175. The Foundation shall be liable for its obligations only with all its assets. The regulations may provide for exceptions to this rule.

176. Foundations may carry out public benefit activities and use public funds.

177. The basis for the foundation activity are the assets provided by the founder. The foundations may also be financed by subsidies from central and local administration, grants from grant-awarding organisations, public collections and donations from individuals and legal entities, the foundation own gainful activity (chargeable public benefit activity, economic activity).

178. Foundations are obliged to keep full accounts. The foundations are supervised by a competent minister (indicated in the Statue). On the other hand, control powers are vested in public institutions that provided grants to a given organisation, and in the case of all subsidies from public funds - in the Supreme Audit Office. If the foundation has the status of a public benefit organisation, it is also supervised by the Minister of Labour and Social Policy. The General Inspector of Financial Information who simultaneously acts as the coordinator of the control, exercises control over the performance by foundations (which are obligated institutions within the meaning of the Act) of their duties in the scope of counteracting money laundering and financing of terrorism as well as: heads of customs and tax control offices, ministers, district governors (Polish: starosta) - within the scope of their supervision or control over the foundation.

179. Once a year each foundation submits a report on its activity to the competent minister and sends it together with the CIT-8 form to the tax office.

180. The foundation may be put into liquidation only in two cases - when the statutory objective has been achieved or when the funds allocated for its activities have been exhausted.

181. According to GUS data, as of 31 December 2018, there were 26,567 foundations[54], i.e. about 1.7% less than a year earlier. The number of registered foundations differs depending on the region of Poland - definitely their highest number was recorded in the Mazowieckie Province (approx. 30.1%)[55].

182. The basic legal act regulating the issues of associations, their founding and functioning is *the Act of 7 April 1989 - The Law on Associations* (Journal of Laws of 2019, item 713).

183. An association is a basic organisational and legal form in which one of the most important constitutional rights guaranteed by the Constitution - the right to freedom of association and joint activities - is implemented. The legal definition of an association as one of the types of civic associations is contained in Article 2(2) of the aforementioned Act. It defines the association as a voluntary, self-governing, sustainable and non-profit making federation. The law on associations does not define the term of federation. The provision only implies that an association is a type of federation whose attributes (such as its voluntary nature, self-governance, sustainability, non-profit goals) are indicated in Article 1 of the Act. The association shall independently determine its objectives, activity programs and organisational structures and adopt internal acts concerning its activity. The activity of an association is based on the social work of its members. The association may employ staff to conduct its affairs, including its members.

184. The association is subject to mandatory entry in the register of associations maintained within the National Court Register. After the entry in the register, the association acquires legal personality. Associations become obligated institutions if they cumulatively meet three conditions:

- if they have legal personality;
- if they were established under *the Act - Law of Associations*;
- they accept or make cash payments of the total value equal to or exceeding the equivalent of EUR 10,000, regardless of whether the payment is performed as a single operation or as several operations which seem linked with each other.

185. The association may be established by at least 7 persons at the founding meeting. These persons become founding members of the association. At the founding meeting, they adopt resolutions on: establishing the organisation, adopting the statute , electing the governing bodies of the association. They may also adopt a resolution to elect a founding committee. After the appointment of the management board, it submits an application to the National Court Register (including the required attachments) for the registration of the association. The association acquires legal personality upon entry in the National Court Register.

[54] Structural changes in the groups of national economy entities in the REGON register, 2018, GUS, Warsaw, 2019, p. 29.

[55] The majority of them were registered in Warsaw, about 80.4% of the foundations registered in the Mazowieckie Province.

186. The non-profit goal of the association is manifested in the assumption that the objective of the association may not be the provision of financial benefits to members of such an association. It does not mean a ban on generating revenue or even generating surplus revenue over costs (profit), however, it is equivalent to an order to allocate this surplus only for statutory purposes of the association and the prohibition of its distribution among its members.

187. The supervision over the activity of associations is exercised by:

- a governor of the province competent for the registered office of the association - with regard to supervision over the activity of associations of local government units,
- a district governor competent for the registered office of the association - with regard to the supervision over associations other than those referred to in the previous subparagraph.

188. The General Inspector of Financial Information who simultaneously acts as the coordinator of the control, exercises control over the performance by the associations (which are obligated institutions within the meaning of the Act) of their duties in the scope of counteracting money laundering and financing of terrorism as well as: heads of customs and tax control offices, governors of provinces or district governors - within the scope of their supervision or control over the association.

189. The assets of the association arise from membership fees, donations, inheritance, bequests, income from own activities, income from the assets of the association and from public generosity. The association may accept donations, inheritance and bequests and benefit from public generosity, in compliance with the applicable regulations.

190. In addition to associations registered in the National Court Register, there are also so-called ordinary associations without legal personality. Three people are sufficient to establish such an association. Ordinary associations do not have to create statute - their activities are carried out under the rules of procedure. They register in the records of ordinary associations (in the office). An ordinary association has no legal personality and it is a so-called "deficient legal entity". It may incur liabilities, sue and be sued. Sources of funding include membership fees and grants but the ordinary association cannot carry out business activity (chargeable or economic).

191. According to GUS data, as of 31 December 2018, there were 114,687 associations and social organisations[56], i.e. approx. 5.2% less than a year earlier. The number of associations differs depending on the region of Poland - their highest number was definitely recorded in the Mazowieckie Province and Wielkopolskie Province (in total, approx. 23.9%).

192. According to the Klon/Jawor Association Report “2018 - Condition of NGOs”, not all registered associations or foundations actually operate. Estimates show that about 65% of registered organisations are active. Thus, there are about 80 thousand active associations and foundations in Poland.[57] In addition, the average association has 30 members, 15 women and 15 men. Out of 30 people, 10 members are actually active, i.e. they are really involved in the

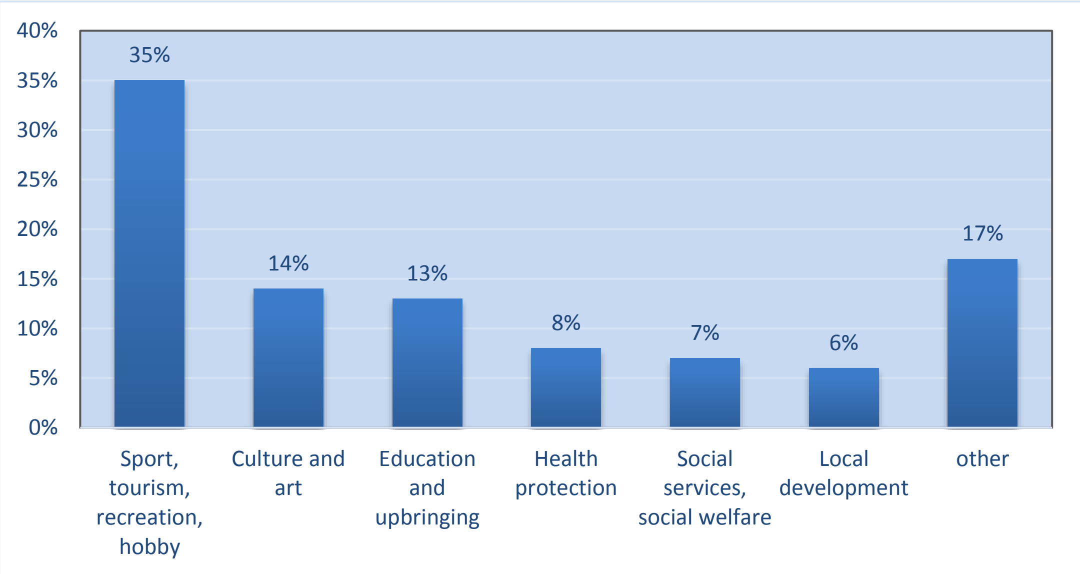
[56] Structural changes in the groups of national economy entities in the REGON register, 2018, GUS, Warsaw, 2019, p. 29.
[57] Based on the data derived from: 2018 - Condition of NGOs, Klon/Jawor Association, Warsaw, February 2019, p. 9, available at: https://fakty.ngo.pl/raporty/kondycja-organizacji-pozarzadowych-2018.

life of the organisation. [58] 63% of organisations engage volunteers, 6 persons per year, on average. Half of them, i.e. 3 persons, operate regularly, at least once a month[59]

193. The average annual budget of the association/foundation in 2017 amounted to approx. PLN 28 thousand. About 30% of the organisations had annual revenues ranging from PLN 1 thousand to PLN 10 thousand (of which even 11% - up to PLN 1 thousand). Most of them were those with revenues in the range of PLN 10,000 and PLN 100,000 (approx. 43%). Revenues above PLN 100,000 and below PLN 1 million were reported by about 22% of associations/foundations. The percentage of organisations with annual revenues exceeding PLN 1 million was relatively low (i.e. approx. 6%).[60]

194. The area of activity of associations and foundations is diversified. The data of the Klon/Jawor Association show that the majority of organisations operate in the field of sports, tourism, recreation, hobbies, culture and arts.

Figure no. 3 - Percentage of organisations operating in individual areas[61]



195. Other areas of activity of the aforementioned organisations include: environmental protection, ecology, labour market, scientific research, maintenance of national identity, law and its protection, human rights, professional matters, rescue activities, security, defence, international activity, development aid, religion or support for non-governmental organisations.

2.2.6. Real estate market

196. The term of real estate in Poland is based on the concept of *res immobiles* developed by Roman law, understood as land and anything permanently connected with it. Pursuant to Article 46 §1 of *the Civil Code* (kc), real property includes: parts of the land area constituting a separate object of ownership (land) as well as buildings permanently connected with the land or parts of such buildings, if they constitute a separate object of ownership under special provisions. On

[58]Ibidem, p. 15.
[59]Ibidem, p. 26.
[60] 2018 - Condition of NGOs, Klon/Jawor Association, Warsaw, February 2019, p. 12, available at:https://fakty.ngo.pl/raporty/kondycja-organizacji-pozarzadowych-2018.
[61]Ibidem, p. 11.

the other hand, pursuant to Article 4 of *the Act of 21 August 1997 on real estate management* (Journal of Laws of 2018, item 2204, as amended), the real estate is land with its components, excluding buildings and premises, if they constitute a separate object of ownership. Taking into account these definitions, there are three types of real estate: land, buildings and premises. Land is always real estate whereas buildings permanently connected with land and parts of such buildings (premises) are separate real properties where it is provided for in the specific provisions. Otherwise, they are the components of the land.

197. Agricultural real estate (agricultural land) is such a land which is or can be used for pursuing manufacturing activity in the scope of plant, animal, horticultural, fruit and fish production. Other land is non-agricultural land.

198. Depending on the criterion adopted, real estate is classified as: agricultural real estate, forest, real estate intended for development, recreation, cemetery, other. According to other criteria, a distinction can be made between: developed, undeveloped, land, buildings, premises consisting of two or more registered plots of land, owned by the State Treasury, local government units, other.

199. The issues of real estate trade in Poland are regulated by *the Act* of *21 August 1997 on real estate management*. In Article 13 the Act stipulates that real estate may be traded. In particular, real estate may be the subject of sale, exchange and relinquishment, letting into perpetual usufruct, rental or lease, lending, letting into permanent management and may be encumbered with limited property rights, submitted as non-cash contributions (in-kind contributions) to companies, transferred as equipment for state enterprises under establishment and as assets of foundations under establishment.

200. Information on the legal status of a real estate is included in the land and mortgage register which is a type of register kept by a public entity. The land and mortgage register contains information about the former and current legal status of the real estate. On the basis of land and mortgage registers it is possible to determine who may dispose of a given property, who is its owner or who has the particular type of rights to such real estate.

201. With respect to land and mortgage registers, the principle of reliability of land and mortgage registers is applied which stipulates that the legal status of real estate disclosed in the land and mortgage register is consistent with the actual legal status.

202. In the event of any discrepancy between the legal status of the real estate disclosed in the land and mortgage register and the actual legal status, the contents of the register shall determine in favour of the person who acquired ownership or other right in rem through a legal action with a person authorised according to the contents of the register.

203. In the Polish legal system, the transfer of ownership of the real estate requires the conclusion of a contract in the form of a notarial deed (Article 158 of the kc). The deed shall be drawn up for the purpose of confirmation, authentication or approval of the particular legal act. By drawing up the notarial deed, the notary also certifies that certain facts have taken place and are lawful. A notary, as a person of public trust, is not the only person who can draw up such a deed. A Polish consul may also exercise such activity abroad, however, only upon a written authorisation of the Minister of Justice at the request of the Minister of Foreign Affairs.

204. Notaries are obligated institutions in the scope of activities performed in the form of a notarial deed, comprising, among others:

- transfer of the ownership of an asset, including sale, exchange or donation of movable property or real estate;
- concluding an agreement on distribution of the estate, dissolution of co-ownership, life annuity, rent in exchange for the transfer of the ownership of an asset and on distribution of jointly-held assets;
- assignment of the cooperative ownership title, title to premises, perpetual usufruct title and alleged promise of a separate ownership of premises.

205. A notary may accept the notary deposit as a form of securing the transaction as defined in Article 108 of *the Act of 14 February 1991 - Law on Notaries.* A notary has the right to accept money (or securities) for safekeeping in connection with a notarial deed executed in his/her office, in order to release it to the specific person - the money may be accepted in a foreign currency or in Polish currency. A notary public should draw up a report on the acceptance of such a deposit. The report is prepared at the customer's request. The notary deposit is usually established during the sale of the property. It is then the security for the buyer who may be afraid to spend the money before receiving the final notarial deed.

206. A real estate intermediary - an entrepreneur conducting business activity in the field of real estate intermediation - may participate in the real estate trade. Real estate intermediation consists in paid performance of activities aimed at concluding by other persons of agreements for the purchase or sale of titles to the real estate, cooperative ownership right to premises, rental or lease of the real estate or parts thereof as well as other activities involving titles to the real estate or parts thereof. The scope of real estate intermediation services is specified in the intermediation contract concluded with the customer. The contract must be executed in writing or in electronic form under pain of invalidity. Each entrepreneur may perform intermediation activities in real estate trading subject to holding a civil liability insurance for damages caused in connection with the performance of these activities.

207. Intermediaries in real estate trading are obligated institutions within the meaning of *the Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism.* The data of the GUS included in the quarterly information on national economy entities show that as of 31 December 2018 in the national official register of national economy REGON (excluding natural persons running only individual farms), 18,548 entities were registered indicating their activity within the scope of the Polish Classification of Business Operations (PKD) - 6831Z, i.e. intermediation in real estate trading[62].

208. One of the banking instruments established pursuant to the so-called *Developer Act*, i.e. *the Act of 16 September 2011 on the protection of the rights of a purchaser of a residential unit or a single-family house* (Journal of Laws of 2017, item 1468 as amended) is the housing trust account. It is an account created under the developer's agreement[63] with a bank, used to collect

[62] https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2018,7,6.html, 19.03.2019

[63] Pursuant to Article 3(1) of *the Act of 16 September 2011 on the protection of the rights of the purchaser of a residential unit or a single-family house*, this term shall mean "an entrepreneur within the meaning of *the Act of 23 April 1964 - Civil Code* (Journal of Laws of 2017, items 459, 933 and 1132) who in the course of its business activity pursued under the development agreement undertakes to establish the title referred to in Article 1 and transfer this right to the purchaser".

funds paid by the buyer of the real estate for purposes defined in the developer agreement. The Act imposes an obligation on developers to open housing trust accounts for each development project[64] and the level of protection of purchasers depends on the type of such account. Future owners of flats or single-family houses transfer funds for the purchase of real estate to the housing trust account. This way of collecting their money is intended to provide better protection. The housing trust account may have a closed or open form. In the first case, the accumulated money is paid out once, after the transfer of ownership of the real estate to the buyer. In the case of an open housing trust account, payment is made on the basis of the development investment schedule specified in the agreement with the bank. This type of housing trust account may be maintained either independently or with additional security in the form of a bank or insurance guarantee.

209. As of the end of 2018 Q2, the total value of household debt in Poland due to housing loans taken out for the first time exceeded the level of PLN 400 billion. The average total value of a housing loan granted in 2018 Q2 amounted to PLN 255,405.[65]

2.2.7. Other market segments

The art market

210. The art market is a specific market. The subject of trade on this market are commodities of specific nature whose economic treatment as a commodity differs from the concepts of standard goods. Works of art, in economic terms, are individual goods, not subject to standardisation, of heterogeneous character. They do not meet many assumptions of economic theories concerning, among others, homogeneity of goods, the law of supply, stability of consumer preferences.

211. The art market faces the fundamental problem related to price formation on this market. The basic problem is the lack of a link between the cost of production and the price of the piece of art. This is mainly affected by the fact that the limitation is the restricted access to data on the art market. For this reason, forecasts are most often made based on the auction market. However, the analyses of price levels carried out using this method do not take into account the considerable primary market segment, sales in art galleries within the secondary market, private auctions and unpublished auction results. The difficulty in pricing works of art is affected by the heterogeneity and uniqueness of the work, the relative rarity of the transaction (compared to traditional financial markets), the limited access to financial data on the art market (the only data available relate to the auction market) and the low liquidity of the object.

---

[64] A development project is defined in Article 3(6) of the so-called *Act of 16 September 2011 on the protection of the rights of the purchaser of a residential unit or a single-family house* as a “process, as a result of which the right referred to in Article 1, comprising the construction within the meaning of the Act of 7 July 1994 - Construction Law (Journal of Laws of 2016, item. 290, 961, 1165, 1250 and 2255) is established or transferred to the buyer as well as factual and legal actions necessary to commence the construction and commissioning of the construction facility and in particular, the acquisition of rights to the real property on which the construction is to be carried out, preparation of the construction project or acquisition of rights to the construction project, acquisition of construction materials and obtaining the required administrative permits specified in separate regulations; an investment task related to one or more buildings may be a part of the development project if, in accordance with the schedule of the development project, these buildings are to be commissioned at the same time and form an architectural and construction whole”.

[65] AMRON-SARFiN report. The national report on housing loans and transaction prices of real estate 2/2018, p. 4, available at: http://www.amron.pl/strona.php?tytul=raporty-amron-sarfin.

212. Auction houses, galleries and antique shops operate as intermediaries on the Polish art market.

213. According to the data contained in the GUS report on the market of works of art and antiques in 2017, based on the information received from 213 entities operating in this area, 117 of them (i.e. 54.9%) were involved in the sale of works of art and antiques, while 96 (i.e. 45.1%) were involved in the sale of works of art and antiques and exhibition activities[66] The total value of sale for works of art and antiques amounted to PLN 138.0 million. The channel most frequently chosen for distribution of works of art and antiques were traditional auctions organized by an individual entity (PLN 65.0 million, i.e. 47.1%). Compared to 2016, the sale of works of art and antiques via the Internet increased by 5.5% (from PLN 11.8 million to PLN 12.4 million).

214. The largest number of the aforementioned entities was located in the Mazowieckie Province, i.e. 50 (23.5%), including 43 in Warsaw. The highest sale of works of art and antiques was recorded in the Mazowieckie Province - 52.4% of the total sales volume. Works of art and antiques in the field of painting were most frequently sold whose share in the total sale volume amounted to 65.0%, including the sale of works of contemporary painting amounting to 50.2%, and for the old painting (performed before 1945) - to 49.8%.

215. Slightly different statistical information is provided by *Artinfo*, a portal dealing with the art market. The main findings of the Report - *Auction market in 2017* are as follows:

- the turnover of auction houses increased by 28% year on year and reached a record high level of PLN 214.1 million;
- the largest number of auctions in history were conducted: 284;
- auctions were organised by 49 entities - auction houses and galleries;
- a new all-time price record time was set - "Motherhood" by Stanisław Wyspiański was auctioned in DesieUnicum for PLN 4,366,000 (during the year 20 transactions over PLN 1 million were concluded);
- the balance in the sales structure (contemporary art 51.5%, old art 48.5%);
- Warsaw remains the most important centre of art auctions (90.6% of turnover);
- painting is the most important group of sold objects (80.3% of market turnover);
- the market is more and more accessible to new participants. Nearly one-third of transactions were performed at prices up to PLN 1 thousand and nearly three-quarters of transactions - at prices up to PLN 5 thousand;
- the most expensive artists who created before 1945: Stanisław Wyspiański, Jan Matejko, Mojżesz Kisling, Józef Chełmoński, Henryk Hayden;
- the most expensive contemporary artists in 2017: Wojciech Fangor, Magdalena Abakanowicz, Ryszard Winiarski, Tadeusz Kantor, Henryk Stażewski, Tadeusz Brzozowski;
- the most expensive artists (young and current art): Sandra Arabska, Daniel Pawłowski, Adam Bakalarz, Wojciech Brewka, Ada Plucha.[67]

[66] Market of works of art and antiques in 2017, GUS, 29 June 2018, pp. 1-3, available at: https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5493/17/2/1/rynek_dziel_sztuki_i_antykow_w_2017.pdf.
[67] http://www.artinfo.pl/pl/publikacje/artinformacje/wyjatkowy-i-rekordowy-rok-2017/?page=3, date of reading 8 May 2019

216. The art market is the largest segment of the alternative investment market, with paintings, sculptures, graphics, posters, porcelain, antiques or applied arts as its subject matter, and demand for works of art depends on the period and place of their creation. The advantage of the art market is its low sensitivity to business cycles. The artwork index which did not surrender to the pressure of the market, clearly rose during periods of economic downturn.

217. One of the services offered by *private banking* is *art banking* which comprises professional advice on collecting works of art. Using this service, the customer receives assistance in the acquisition of works of art, their valuation or authentication. The Bank assesses the technical condition of a work of art and the current situation on the art market. Within the framework of the *art banking* offer, the bank also represents the client in auctions, negotiates the price and other terms of the transaction. In addition, it ensures safe transport, storage, insurance and maintenance of exhibits. However, the use of non-financial services such as *art banking* in Poland is not yet as widespread as in the case of foreign institutions. Banks limit themselves to simple management of the client's assets, increased by alternative investments. Polish *art banking* lacks, among others, loans collateralised by works of art, loans for their purchase as well as professional advice on the art market. The *art banking* offer within the Polish *private banking* offer comprises mainly painting whereas in other countries it also focuses on sculpture, photography, posters and cartoon boards. In Poland, *art banking* is not yet popular as a form of capital investment.

Safe Deposit Boxes

218. The safekeeping of objects and securities is regulated by the provisions of *the Civil Code* (Articles 835-845). Its subject matter is the releasing of movable property for safekeeping to the depositary (custodian) free of charge or against remuneration. The custodian shall be bound to maintain the item deposited in a condition that is not deteriorated and to deliver it at any time at the request of the depositor. When securities are held in custody, it is important that they are marked in terms of their identity and in traditional (i.e. not dematerialised) form. Otherwise, it is difficult to refer to storing securities which cannot be physically stored. Banks provide object storage services as institutions of public trust.

219. In accordance with Article 5(2)(6) of *the Act of 29 August 1997 - Banking Law*, banking activities include providing access to a safe-deposit box, provided that such activities are performed by banks. The safe deposit box agreement in this respect is similar to the storage agreement. In such agreement, the bank undertakes, against payment, to make available a safe-deposit box to its counterparty, adequately secured and excluded from the third party access. It is designed to hold valuables.

220. Safe-deposit boxes are provided by banks almost exclusively within the framework of the so-called *private banking*. However, not all banks offer this type of service[68] In order to provide access to safe deposit boxes, additional space must be provided and the rooms must be adequately secured. Stronger safeguards also increase costs. The price of safe deposit box rental depends on the size of the safe and the lease period. As a rule, it is lower in banks than in specialised companies providing access to safe-deposit boxes.

[68] In 2018, the UKNF (PFSA) conducted an inspection in 12 commercial banks in order to verify the compliance with the obligations related to the provision of safe deposit box services.

221. The services of providing safe deposit boxes by banks may be used by both adult natural persons, legal persons and even organisational units without legal personality. Banks provide lockers for both residents and non-residents, i.e. persons residing abroad. A foreigner may use a safe-deposit box on the basis of a valid passport, while a Polish citizen may use a safe-deposit box on the basis of an identity card.

222. The safe deposit box agreement and related regulations strictly define which items may be placed in the safe deposit box. These can include securities, important documents, jewellery, works of art, precious metals, small collector's items (stamps, coins) or other valuable items. Explosive and radioactive substances, weapons, drugs, perishable articles and objects derived from crime are excluded. Attempting to place such items in a bank deposit may provide grounds for termination of the agreement.

223. The Bank is bound to provide information constituting bank secrecy, including information on the safe deposit boxes that have been made available, only to authorised entities indicated in the provisions of *the Act of 29 August 1997. - Banking law* (including prosecutor's offices, the police, the National Revenue Administration (KAS), Central Anti-Corruption Bureau (CBA), Internal Security Agency (ABW)). In addition, the contents of the box may be made available to a bailiff acting pursuant to the court enforcement order.

224. If the term of the agreement expires and the tenant does not pay for the extension, the bank has the right to empty the safe-deposit box. However, it shall calls upon the customer in advance to return the key to the safe-deposit box and empty it and in the event that the call is ineffective, it empties the contents of the safe-deposit box and deposits it in another place until it is collected by the former tenant.

225. Providing access to safe deposit boxes may also be a subject of business activity within the meaning of *the Act of 6 March 2018 - Entrepreneur law*. Entrepreneurs operating pursuant to the provisions of the aforementioned Act, to the extent they conduct activities consisting in providing access to safe-deposit boxes and branches of foreign entrepreneurs conducting such activities in the territory of the Republic of Poland are obligated institutions within the meaning of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*.[69]

[69] It is possible to find offers from at least a few non-bank entities offering services in this area on the Internet.

3. DESCRIPTION OF MONEY LAUNDERING AND TERRORIST FINANCING PHENOMENA

3.1. MONEY LAUNDERING

226. [In Polish] the term "pranie pieniędzy" is a literal translation of the English term "money laundering". Initially, it was correlated with introducing money originating from criminal activities into circulation through economic activities (e.g. through ordinary money laundries) in order to ensure its legitimate use. Currently, the meaning of this term covers a wide range of activities related to the transfer of possession or ownership of assets derived from benefits related to committing of a prohibited act, including aiding, abetting, attempting its committing and inciting to commit it. In Article 9(1) of *the Council of Europe Convention of 16 May 2005 on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism* (ratified by Poland - Journal of Laws of 2008, No. 165, item 1028)[70] known as the Warsaw Convention, money laundering is defined as an intentional action aimed at:

- the conversion or transfer of property, knowing that such property is proceeds, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is proceeds;
- the acquisition, possession or use of the aforementioned property;
- participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the aforementioned offences.

227. The first Polish legal regulations related to combating money laundering appeared at the beginning of the 1990s. They included ordinances of the President of the National Bank of Poland:

- *ordinance No. 16/92 of the President of the National Bank of Poland of 1 October 1992 regarding the rules of conduct of banks in the event of disclosure of circumstances indicating that funds or other assets originating from or related to crime are invested in a bank and that cash payments are made in excess of a specified amount* (Official Journal of the NBP No. 9, item 20);
- *ordinance No. C/2/I/94 of the President of the National Bank of Poland of 17 January 1994 on preventing the use of the activities of NBP organisational units to perform activities aimed at concealing the origin of funds from or related to crime*.

228. The definition of the offence of money laundering and sanctions for its committing were defined for the first time under the Polish law in the *Act of 12 October 1994 on the protection of economic turnover and amendment of certain provisions of the criminal law* (Journal of Laws

[70] The Convention was ratified by Poland on 8 August 2007 and entered into force on 1 May 2008.

of 126 item 615). It identifies a narrow catalogue of possible predicate offences[71] related to organised crime. Money laundering in the first version of Article 299 of *the Act of 6 June 1997 - Penal Code* was described in a similar way. (Journal of Laws of 2018, item 1600 as amended).

229. An interesting definition of money laundering was introduced by *the Act of 5 March 2004 amending the Act on counteracting the introduction to financial trade of property values derived from illegal or undisclosed sources and on counteracting the financing of terrorism and amending certain acts* (Journal of Laws No. 62, item 577), however, it was not directly related to the content of the then binding provision of *the Penal Code*, hereinafter referred to as the kk, which penalises money laundering (Article 299 of the kk). The aforementioned Act indicated that the introduction to financial trade of property values coming from illegal or undisclosed sources should be understood as “an intentional proceeding consisting in

a) the conversion or transfer of assets[72] derived from criminal activity or from an act of participation in such activity, in order to conceal or disguise the illicit origin of such assets or to assist a person who takes part in such activity to evade the legal consequences of such activity;

b) concealing or disguising the true nature, source, place of storage, fact of transfer or rights attached to property values derived from criminal activity or participation in such activity;

c) the acquisition, taking possession or use of assets derived from criminal activities or from participation in such activities;

d) co-operation, attempt to commit, aiding or abetting in case of any of the conduct referred to in subparagraphs (a) to (c);

- also if the activities under which the property values being the subject of the introduction to financial trading of the values coming from illegal or undisclosed sources were obtained were carried out on the territory of another state”[73].

230. At the same time, the following activities were indicated as basic activities in the framework of money laundering:

- conversion of property values;
- their transfer;
- purchase;
- acquisition of the possession;
- use.

[71] The concept of the predicate offence refers to punishable acts which may give rise to property gains subject to laundering. It was also defined in Article 1(e) of *the Council of Europe Convention of 16 May 2005 on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism* as any offence which gives rise to proceeds liable to be subject to a money laundering offence.
[72] Defined then as means of payment, securities or foreign exchange values, property rights, movable and immovable property.
[73] The concept of “introduction to financial trading of assets coming from illegal or undisclosed sources” was amended by *the Act of 25 June 2009 amending the Act on counteracting the introduction to financial trading of assets coming from illegal or undisclosed sources and on counteracting terrorist financing and amending certain other acts* (Journal of Laws No. 166, item 1317) to “money laundering”. This legal act introduced minor adjustments to subparagraph b and to the common sentence for all subparagraphs of this definition.

231. The above mentioned activities were linked to five fundamental rules:

1) The subject of the activities are or shall be assets derived “from criminal activity or from participation in such activity”.
2) The perpetrator is aware of the illegal origin of the aforementioned property values.
3) The purpose of the above mentioned activities is to hide or conceal the illegal origin of property values or their nature, as well as their source, place of storage, disposal, and the fact of their transfer.
4) Activities undertaken for the above mentioned purpose shall also include: cooperation, attempt to commit the offences, aiding or abetting.
5) The predicate offence for money laundering may be committed both within and outside the territory of Poland.

232. At present, in the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the notion of money laundering is defined by reference to Article 299 of the kk. In accordance with this criminal provision, money laundering shall be understood as:

- receiving, possessing, using, transferring or exporting abroad, concealing, transferring or converting means of payment, financial instruments, securities, foreign exchange values, property rights or other movable property or real estate derived from proceeds related to committing a prohibited act;
- assisting in the transfer of ownership or possession of the aforementioned property values;
- undertaking other activities which may prevent or significantly hinder the determination of the criminal origin or location of placement of the aforementioned property values, their detection, seizure or forfeiture.

3.2. FINANCING OF TERRORISM

233. Since the events of 11 September 2001, counteracting money laundering has been closely associated with combating financing of terrorism. This relationship is based, in particular, on two facts:

- terrorist activities are often financed by profits from illegal activities;
- for financing of terrorism similar methods of procedure are used (including money transfer) as in the case of money laundering.

234. There are different definitions of terrorism, to which many scientific studies have been devoted. The main reason for this is that terrorism is commonly identified with the means used, i.e. violence on a relatively large scale. For this reason, the term is often defined as the specific method of operation rather than a separate, comprehensive political phenomenon[74] In principle, certain common parts can be distinguished, found in the majority of terrorism definitions:

- perpetrators of terrorist acts: extremists;

[74] Damian Szlachter, Fight against Terrorism in the European Union - a new impulse, ed. Adam Marszałek, Warsaw 2007, p. 22

- the method they use: violence or the threat of using violence;
- recipient of terrorist acts: the public or its part, the authorities of the country/countries concerned, international institutions and organisations;
- indirect target of the perpetrators: intimidating the recipient;
- the main objective of the perpetrators: to achieve political concessions.

235. Contrary to the definition of terrorism, the concept of financing of terrorism is easier to formulate. In principle, the majority of its definitions resemble the definition presented in *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* (OJ L 141, 05.06.2015, p. 73). The aforementioned Directive indicates that "«terrorist financing» shall mean the direct or indirect supply or collection of funds, by any means, with the intention that they should be used, or with knowledge that they are to be used, in full or in a part, to commit any of the offences referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA".[75]

236. *The Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, implementing the provisions of the above mentioned directive, defines financing of terrorism by reference to Article 165a of the kk.

237. The current wording of Article 165a of the kk describes in detail the behaviour defined as financing of terrorism. In accordance with this provision, it comprises:

- collecting, transferring or offering means of payment, financial instruments, securities, foreign exchange values, property rights or other movable property or real estate with the intention to finance offences of terrorist nature[76] or the offences referred to in Article 120, Article 121, Article 136, Article 166, Article 167, Article 171, Article 252, Article 255a or Article 259a of the kk,
- making the aforementioned property available to an organised group or association aiming to commit the aforementioned offences or to a person participating in such a group or association or to a person who intends to commit the aforementioned offences,
- covering costs related to meeting the needs or financial obligations of the above mentioned group, association or person,

238. At the same time, it was pointed out that that provision penalises the aforementioned actions undertaken both intentionally and unintentionally.

---

[75] This concept is similarly defined in *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* (OJ L 309, 25.11.2005). "Terrorist financing shall mean the direct or indirect supply or collection of funds, by any means, with the intention of their use or with awareness that they are to be used, fully or partially, in order to commit any of the offences referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism".

[76] The terrorist offence is defined in Article 115 § 20 of the kk.

4. COUNTERACTING MONEY LAUNDERING AND FINANCING OF TERRORISM

4.1. A BRIEF HISTORICAL BACKGROUND

239. On 16 December 1991, an international agreement on the association of Poland with the European Communities and their Member States, known as the Agreement, was signed in Brussels. Poland was then committed to adjust its money laundering legislation to the requirements of the European Union. It became necessary to take steps in order to ensure the compliance of the national legislation with *Directive of the Council of the European Communities of 10 June 1991 on the protection of the use of the financial system for the purpose of money laundering* and the requirements of the Vienna Convention *on Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, ratified in 1994. The establishment of the office of the General Inspector of Financial Information has also become a priority of the National Programme of Preparations for Polish EU Membership and the Partnership for EU Membership.

240. Immediately after signing the association agreement, the National Bank of Poland played an active role in preventing money laundering by implementing the *Ordinance No. 16/92 of the President of the National Bank of Poland of 1 October 1, 1992, of the President of the National Bank of Poland of 1 October 1992 regarding the rules of conduct of banks in the event of disclosure of circumstances indicating that funds or other assets originating from or related to crime are invested in a bank and that cash payments are made in excess of a specified amount* (Official Journal of the NBP No. 18, item 40) constituting the basis for building a national anti-money laundering system. Money laundering was criminalised by including Article 5 in the *Act of 12 October 1994 on the protection of economic turnover and on the amendment of certain provisions of criminal law* (Journal of Laws No. 126, item 615). Subsequently, in *the Penal Code of* 1997, Article 299 of the kk was included, and in the *Banking Law* - Article 106-108.

241. Starting from 1995, various concepts for the location of the anti-money laundering unit were put forward in Poland. In 1998, the idea was put forward to establish the State Financial Information Agency as a central body of state administration. In the same year, the Ministry of Internal Affairs and Administration (MSWiA) attempted to establish an organisational unit, which in December 1998 took the form of the National Centre for Financial Information, within the framework of which the Financial Information Department was established. In 1999, the aforementioned Centre, which remained within the structure of the Ministry of Internal Affairs and Administration as a department, was dissolved. Subsequently, the concept of appointing the General Inspector of Financial Information (GIFI) as a governmental agency within the structure of the Ministry of Finance was finally adopted.

242. A breakthrough was the adoption of *the Act of 16 November 2000* on *counteracting the introduction to financial trading of property values derived from illegal or undisclosed sources.*

The basic assumption of the aforementioned Act was to establish a government administration body called the General Inspector of Financial Information (GIFI), in order to collect, process and analyse financial information for detecting suspicious transactions. An internal organisational unit of the Ministry of Finance - Financial Information Department - was designated to assist in the implementation of its statutory tasks.

243. The adoption of the aforementioned Act started a new stage in the fight against the money laundering procedure. On 21 February 2001, pursuant to Article 3(2) and (3) of the aforementioned Act, the Prime Minister appointed the first GIFI**.** Tasks reserved for the GIFI included the cooperation with similar foreign institutions in the field of exchange of experience and information for the detection of the money laundering practice. The Financial Information Department of the Ministry of Finance was established pursuant to the *Ordinance No. 2 of the Ministry of Finance of 23 March 2001 amending the Ordinance on introduction of the Ministry of Finance organisational rules*. Its structure was determined by *Ordinance No. 1 of the Director of the Financial Information Department of 28 May 2001 regarding the introduction of the internal regulations of the Financial Information Department.*

244. The amendment to the aforementioned Act submitted in March 2002 was connected with the fact that the said project of counteracting the financing of terrorism was covered by the said draft. The introduction of regulations related to this subject is one of the elements to implement the provisions of *UN Security Council Resolution 1373 (2001) on combating international terrorism and the recommendations of the Financial Action Task Force on Money Laundering operating under the auspices of the OECD* (FATF).

245. Under the next amendment, which was adopted by *the Act of 25 June 2009 amending the Act on counteracting the introduction to financial trading of property values coming from illegal or undisclosed sources and on counteracting the financing of terrorism and amending certain other acts* (Journal of Laws No. 166, item 1317), among others, the name of the Act itself was changed and it was given a new shorter title: “on counteracting money laundering and financing of terrorism”. This Act also introduced to the *Penal Code* a definition and penalisation of behaviour defined as the financing of a terrorist offence (Article 165a of the kk).

4.2. APPLICABLE REGULATIONS

246. The basic legal act relating to the prevention of money laundering and financing of terrorism is the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*. It implements the provisions of *Directive of the European Parliament and of the Council (EU) no. 2015/849 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* (OJ L 141, 05.06.2015, p. 73), hereinafter referred to as Directive 2015/849. First of all, it defines the tasks and powers of the GIFI, as well as the functioning of the Financial Security Committee, the principles of cooperation of the GIFI with cooperating units, and the obligations of obligated institutions.

247. The above mentioned law provides for the issuance of 9 implementing[77] orders, specifying such issues as:

- the manner in which information on transactions and suspicious activity, above-threshold transactions, as well as identification forms, shall be drawn up and provided by the obligated institutions;
- the manner in which information is drawn up, provided and the manner in which prosecutors are to provide information on whether to issue the order on blocking of an account or the suspension of transactions, to initiate proceedings, to present charges and indictment in cases of money laundering or financing of terrorism offences, hereinafter referred to as "information" and by cooperating units to notify suspicions of money laundering or financing of terrorism offences, hereinafter referred to as "notifications";
- the manner of preparing information by the KAS and Border Guard authorities on the import of cash on the territory of the Republic of Poland or its export from the territory of the Republic of Poland, as well as the manner and procedure of submitting such information to the GIFI;
- the method of preparing and submitting by an obligated institution to the GIFI a notification about a case of reasonable suspicion that a transaction or property values may be related to money laundering or financing of terrorism, a notification about the execution of the above transaction, due to the impossibility of making an appropriate notification before its execution, information about notifications submitted to the prosecutor in the case of a reasonable suspicion that a given transaction or property values may be related to a fiscal crime or crime other than money laundering or financing of terrorism, and provisions of the prosecutor issued in connection with such a notification;
- the method of preparing and providing by the GIFI to the obligated institutions the confirmation of receipt of the notification on a justified suspicion that a transaction or property values may be related to money laundering or terrorist financing, a notification on the execution of the aforementioned transaction, requests to suspend a transaction or block an account, exemptions from the obligation to refrain from executing a transaction;
- the manner of accepting by the GIFI of reports concerning real or potential infringements of the provisions in the scope of counteracting money laundering and financing of terrorism from employees, former employees of obligated institutions or other persons who perform or performed activities in favour of the obligated institutions on the basis other than employment relationship;
- the manner and procedure for reporting information on beneficial owners to the Central Register of Beneficial Owners (CRBO);
- the manner in which requests for information from the CRBO are prepared, and the manner and procedure for the submission of such requests;

[77] Statutory delegations referred to in Articles 62, 71, 78(3), 80(3), 85(4) and 134(2), 79(3), 84(4) and 84(4) of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*.

- a specimen of the GIFI controller's service card together with a description of the applied security features of the document.

248. In addition, the aforementioned Act provides for the possibility of issuing by the minister competent for public finance of an implementing regulation[78] specifying the method related to:

- preparing and accepting requests of prosecutors and courts to the GIFI for information and documents for the purposes of criminal proceedings as well as motions of other entities entitled to receive information held by the GIFI;
- providing information by GIFI to investigative bodies other than prosecutors about the suspicion of committing a fiscal offence or an offence other than money laundering or financing of terrorism, as well as information to the KNF (PFSA) in case of a justified suspicion of violation of regulations related to the functioning of the financial market.

249. Apart from the aforementioned Act, EU regulations directly applicable in the territory of the Member States are also of great importance for the functioning of the national anti-money laundering and counter-terrorist financing system. In particular, it refers to such provisions defining the tasks of public administration bodies and the private sector, as:

- *Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006* (OJ L L 141, 05.06.2015, p. 1),
- *EU Council Decision 2000/642/JHA of 17 October*

  2000 concerning arrangements for cooperation between financial intelligence units of the

  Member States in respect of exchanging information. (OJ L 271, 24.10.2000, p. 4).[79]

250. Moreover, the functioning of the national anti-money laundering and counter-terrorist financing system is also affected by national legal acts defining the powers and tasks of particular public administration bodies dealing with combating crime or supervision over the activity of obligated institutions.

4.3. ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING SYSTEM IN POLAND

251. The anti-money laundering and counter-terrorist financing system in Poland consists of:

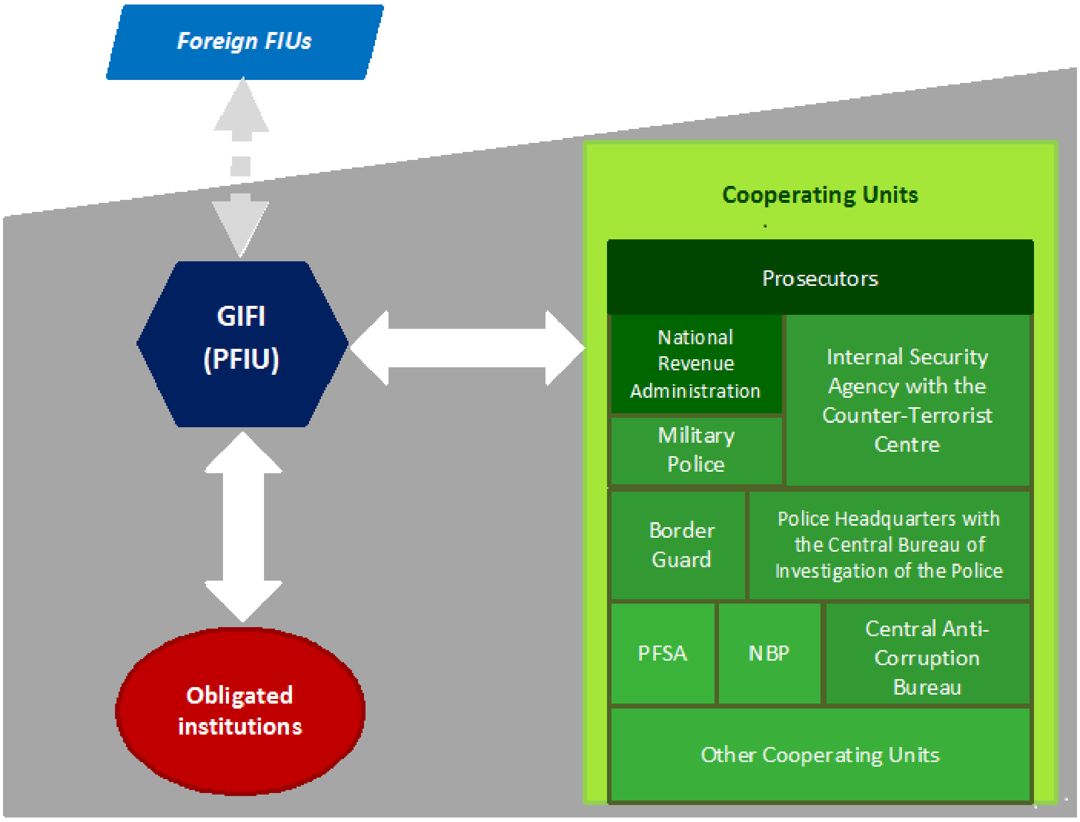
- the GIFI;
- obligated institutions;

[78]Statutory delegation for the optional issue of a regulation as referred to in Article 109 of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing.*

[79]In April 2018, the European Commission presented a proposal concerning the *Directive of the European Parliament and of the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA*. Its first reading by the European Parliament took place in April 2019 (cf.: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0418_EN.html#title1 , date of reading 29 June 2019

- cooperating units.

Figure No. 4 - Scheme of the Polish anti-money laundering and counter-terrorist financing system



4.3.1. General Inspector of Financial Information

252. The central element of the national anti-money laundering and counter-terrorist financing system is the GIFI.

253. Pursuant to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, government administration bodies competent in matters related to counteracting money laundering and financing of terrorism include:

- the minister competent for public finance, as the supreme financial information authority;
- the GIFI.

254. The GIFI is currently appointed and dismissed by the Prime Minister at the request of the minister competent for public finance after seeking the opinion of the minister - member of the Council of Ministers competent for coordination of the activity of special forces, if appointed by the Prime Minister. The GIFI is the Secretary or Undersecretary of State in the office servicing the minister competent for public finance. In the performance of its tasks, the GIFI is supported by the Financial Information Department of the Ministry of Finance playing jointly the role of the Polish financial intelligence unit[80].

255. The tasks of the GIFI include processing information according to the procedure defined in the Act and undertaking measures to counteract money laundering and financing of terrorism, in particular:

- analysing information related to assets, in relation to which the General Inspector has become reasonably suspicious that it is associated with the crime of money laundering or financing of terrorism;
- carrying out of the procedure of transaction suspension or bank account blocking;
- requesting submission of information on transactions and disclosure thereof;
- submission of information and documentation justifying the suspicion concerning the commitment for criminal offence to authorised bodies;
- exchange of information with cooperating units;
- preparing the national money laundering and financing of terrorism risk assessment and strategies on counteracting such criminal offence, in cooperation with cooperating units and obligated institutions;
- monitoring the compliance with regulations on counteracting money laundering and financing of terrorism;

[80] "Financial Intelligence Unit (hereinafter referred to as the "FIU") means a central, state-owned agency responsible for receiving (and, if permitted, providing), analysing and communicating to the relevant authorities of disclosed financial information :

i) concerning suspicious revenues and potential terrorist financing, or

ii) required by national legislation or regulations to combat money laundering and terrorist financing."

pursuant to Article 1(f) of the *Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism* (Journal of Laws of 2008 No. 165, item 1028).

- issuing decisions concerning entering in the list of persons and entities towards which special restrictive measures referred are used, or their deleting from the list as well as keeping this list;
- cooperation with competent authorities of other countries as well as foreign institutions and international organisations dealing with anti-money laundering or combating financing of terrorism;
- imposing administrative penalties referred to in the Act;
- making information and knowledge in the scope of counteracting money laundering and financing of terrorism available in the Public Information Bulletin on the website of the Ministry of Finance;
- initiating other measures to counteract money laundering and financing of terrorism

256. One of the important tasks of the GIFI is the exchange of information with foreign counterparts, i.e. financial intelligences units (FIUs).

257. Until the time of entry into force of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the following acts of law provided grounds for information exchange with the FIUs:

- *EU Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information*. (OJ L 271, 24.10.2000, p. 4), relating to the principles of cooperation within the EU;
- bilateral agreements signed by the GIFI with the FIUs (pursuant to Article 33(5) of the *Act of 16 November 2000 on counteracting money laundering and financing of terrorism* - Journal of Laws of 2017, item 1049)[81];
- the Warsaw Convention.

258. In accordance with the aforementioned Decision, EU Member States shall ensure that the FIU "exchange any available information among themselves, on their own initiative or upon request, on the basis of this Decision or on the basis of existing or future Memoranda of Understanding, which could relate to the processing or analysis of information or to the initiation of an investigation into financial transactions related to money laundering and the natural or legal persons involved"' It also provided for the possibility of refusing to provide information if its disclosure:

- could be detrimental to criminal investigations in an EU Member State;
- would be clearly disproportionate to the substantiated claims of the natural or legal person or the EU Member State concerned;
- would be incompatible with the fundamental principles of national law.

[81] "Information related to the introduction into the financial system of assets derived from money laundering and terrorist financing may be made available by the General Inspector to foreign institutions referred to in Article 4(1)(8) [i.e. "foreign institutions and international organisations dealing with counteracting money laundering or terrorist financing"], on a reciprocal basis, in accordance with the procedure laid down in bilateral agreements concluded by the General Inspector, also by means of computer data carriers".

259. The above-mentioned decision is also binding on Gibraltar.

260. As of December 31, 2018 the GIFI had signed 92 bilateral agreements on the exchange of information with other FIUs. Some of these agreements were signed with the FIUs from EU Member States (most of them still before Poland's accession to the EU).

Table 4 - List of countries whose FIUs has signed information exchange agreements with the GIFI

Europe		**Asia**	**America**	**Africa**	**Australia and Oceania**
Albania	Latvia	Saudi Arabia	Antigua and Barbuda	Algeria	Australia
Andorra	Macedonia	Bahrain	Argentina	Egypt	New Zealand
Armenia	Moldova	Bangladesh	Aruba	Mauritius	
Belgium	Monaco	China	Bahamas	RSA	
Belarus	Germany	Philippines	Belize	Seychelles	
Bulgaria	Norway	Hongkong	Brazil	Tanzania	
Croatia	Portugal	India	British Virgin Islands	Tunisia	
Cyprus	Russia	Indonesia	Chile		
Montenegro	Romania	Israel	Curaçao		
Czech Republic	San Marino	Japan	Cayman Islands		
Estonia	Serbia	Jordan	Canada		
Finland	Slovakia	Qatar	Columbia		
Gibraltar	Slovenia	Kazakhstan	Mexico		
Georgia	Switzerland	Kyrgyzstan	Panama		
Guernsey	Turkey	South Korea	Paraguay		
Spain	Ukraine	Lebanon	Peru		
Ireland	Vatican	Singapore	Saint Vincent and Grenadines		
Iceland	Great Britain	Tajikistan	Sint Maarten		
Jersey	Italy	Thailand	USA		
Kosovo	Man Island	Taiwan			
Liechtenstein		Uzbekistan			
Lithuania		United Arab Emirates			

261. The lack of concluded agreement resulted in the necessity to refuse to provide information in case of inquiries from non-EU FIU (except in the case where the FIU was located in a country which ratified the Warsaw Convention).

262. The main pillars of cooperation in the scope of exchange of information on the basis of the above mentioned agreements are:

- the principle of reciprocity[82];

[82] In accordance with the 2013 "Egmont Group of Financial Intelligence Units Operational Guidance for FIU Activities and the Exchange of Information." (revised in 2017), reciprocity does not address the fact that FIUs

- justification of the request referring to money laundering or financing of terrorism;
- provision of available information and the entities involved in it;
- using information received from another FIU on the terms and for the purposes specified by it;
- refraining from the transfer of information or documents to a third party without the written consent of the FIU from which the information or documents were obtained;
- the FIU is not obligated to provide information if the judicial proceedings have been initiated in the case.

263. Additionally, the GIFI may exchange information (both in the previous legal status and at present) with the FIUs whose countries have ratified the Warsaw Convention. The above-mentioned document, ratified by Poland, provides that the FIU "shall exchange among themselves, on their own initiative or upon request, in accordance with this Convention or with existing or future Memoranda of Understanding consistent with this Convention, all available information which may be relevant for the processing or analysis of information or, where appropriate, for the conduct of investigations by the FIU relating to financial transactions associated with money laundering and related legal or natural persons". Until 26 March 2018, the Warsaw Convention was ratified by 34 countries. Of these countries (excluding the EU Member States), only the FIUs from Azerbaijan and Bosnia and Herzegovina did not have any memoranda with the GIFI.

264. The currently binding *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* regulates in detail the issues related to the exchange of information with foreign FIUs, in accordance with Directive 2015/849. In principle, the provisions of the aforementioned Act indicate that the cooperation in this respect is based on making available to foreign FIUs by the GIFI at their request or ex officio as well as on obtaining from these units information related to money laundering or financing of terrorism, including information on predicate offences from which property values may originate. They clearly indicate that the provisions determining the rules of releasing information covered by legally protected secrets, except for the provisions of *the Act of 5 August 2010 on the protection of classified information*, are not applied. Moreover, the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* do not require signing of a bilateral agreement with a foreign FIU in order to exchange information[83] The agreements signed so far remain in force.

265. The aforementioned Act introduced minor differences between the exchange of information with the FIUs from EU Member States and the exchange of information with the FIUs from other countries. In the first case, the GIFI shall make available to them the information and documents it holds without verifying whether reciprocity has been respected[84]. Additionally, it was obliged to use for this purpose secure communication systems and ICT systems enabling the comparison of the GIFI data with the data possessed by these units in an

have different powers to access various types of information. First of all, the FIUs involved in the exchange of information should be able to provide financial, criminal and administrative information on the basis of their powers. They do not need to have access to the same categories of information.

[83] Such an agreement may be signed if the national legislation of the other Party so requires or if there is a need to clarify the modalities and technical conditions for the exchange of information.

[84] The lack of reference to this rule results from the fact that the FIUs from EU Member States are obliged to implement the same rules of cooperation as specified in Directive 2015/849.

anonymous manner and ensuring personal data protection (i.e. the currently operating IT system FIU.NET and *ma3tch* technology[85]). Moreover, on an ex officio basis, the GIFI shall transmit to the FIU of another EU Member State information concerning that country (e.g. its residents, transactions carried out by resident institutions) and received from obligated institutions concerning:

- circumstances which may indicate the suspicion of committing an offence of money laundering or financing of terrorism;
- reasonable suspicion that the transaction or property values may be related to money laundering or financing of terrorism;
- notification of the prosecutor of any case of reasonable suspicion that the specific assets subject to transaction or collected on the account originate from a crime other than the crime of money laundering or financing of terrorism or a fiscal crime, or are associated with an offence other than the offence of money laundering or financing of terrorism or a fiscal offence.

266. On the other hand, the GIFI shall provide the information available to the FIU of other non-EU Member States on a reciprocal basis. At the same time, the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* clearly indicates that the provisions of the Convention apply to the exchange of information with the FIU from the States-Parties to the Warsaw Convention[86].

267. The GIFI uses primarily *Egmont Secure Web* (ESW), i.e. the IT system developed within the Egmont Group[87] and used by FIU members of the Egmont Group, to exchange information with non-EU FIU.

268. Additionally, besides providing access to information it holds, the GIFI may obtain additional information (e.g. from obligated institutions or cooperating entities) in order to transfer it to the foreign FIUs.

269. The provisions of the aforementioned Act also define the scope of information which should be included in the request for information submitted by the GIFI to a foreign FIU, including:

- identification data of suspected entities[88];

---

[85] FIU.NET and *ma3tch* technology were also used in the previous legal status.

[86] The rules for this exchange are laid down in Article 46 of the Warsaw Convention. They correspond (in particular with regard to the scope of the information exchanged, the purpose of its use, situations that determine the refusal to make it available) to the principles set out in the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*.

[87] The Egmont Group was established in 1995 as an informal international organisation, bringing together the FIUs acting in the scope of promoting and strengthening international cooperation in counteracting money laundering and financing of terrorism. As part of its work, basic standards for the exchange of information between its members were developed and an ICT system was launched to achieve this goal. In 2007, it was turned into a formal international organisation with its own secretariat and staff. As of 15 April 2019, the Egmont Group associated the FIUs from 159 jurisdictions.

[88] Article 112(1) of the aforementioned Act indicates that the scope of such data should be consistent with the scope of data specified for institutions applying customer due diligence measures, i.e. in accordance with Article 36(1) of the Act it should include:

1) In case of a natural person - name and surname, citizenship, PESEL number or date of birth with indication of the country of birth, series and number of a document confirming the identity of the person, address of

- description of the circumstances indicating a link with money laundering or financing of terrorism;
- the intended purpose of the use of the information.

270. Moreover, it is expected that a request for information addressed to the GIFI by a foreign FIU should also contain such information. If it does not comply with those requirements or if it does not sufficiently demonstrate the link between the information requested and money laundering or financing of terrorism, the GIFI shall request that it should be supplemented[89].

271. Upon a justified request from a foreign FIU, the GIFI may allow for the provision of information made available by it to other authorities or the FIUs or the use of such information for purposes other than those related to the tasks of the FIUs. Similarly, the GIFI also applies to foreign FIUs for permission to transfer information received from it to courts, prosecutors and other cooperating units, other FIUs or to use such information for purposes other than the performance of its tasks.

272. Additionally, the GIFI may also demand that a transaction is suspended or the account is blocked upon a justified request of a foreign FIU "enabling to confirm the suspicion of committing a crime of money laundering or financing of terrorism".

273. *The Act of 1 March 2018 on counteracting money laundering and financing of terrorism* also indicates possible situations when the GIFI may refuse to provide information at the request of a foreign FIU:

- the request proposal does not relate to information associated with suspected money laundering or financing of terrorism or the information obtained is to be used for purposes other than the performance of the tasks assigned to the FIU (except where the GIFI has agreed to its use for those purposes);
- requested information is subject to protection in accordance with the provisions on the protection of classified information;

---

residence (in case of possession of such information), as well as - in case of conducting business activity - name (company), the NIP (Tax Identification Number) and address of the main place of business activity.

2) In case of a legal person or an organisational unit without legal personality - name (company), organisational form, address of the registered office or business address, Tax Identification Number (or in the absence of such number - country of registration in the commercial register and number and date of registration), name and surname and PESEL number or date of birth together with indication of the country of birth of the natural person representing the legal person or an organisational unit without legal personality.

It should be noted, however, that the requests addressed by the GIFI will largely be based on information contained in *suspicious activity reports* (SARs) submitted by obligated institutions, which in turn - in accordance with Article 74(3)(2) and Article 86(2) of the aforementioned Act - include only the held data of natural and legal persons and organisational units without legal personality that are not clients of the obligated institution but are involved in suspicious activity. The same applies to the SARs submitted to the GIFI by cooperating entities, which also - in accordance with Article 83(2)(1) of the aforementioned Act - contain "the held data referred to in Article 36(1), natural persons, legal persons or organisational units without legal personality which are related to circumstances that may indicate a suspicion of committing a crime of money laundering or terrorist financing". Therefore, in practice, it will often not be possible for the GIFI to provide the foreign FIU with the full set of data specified in Article 36(1) of the aforementioned Act in the request.

[89] However, it was pointed out that also the request of a foreign FIU to the GIFI should contain identification data within the scope indicated in Article 36(1) of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*, it should be understood that it indicates the identification data held by a foreign FIU (just like the GIFI, a foreign FIU may not have the full set of data specified in this provision).

- making information available could jeopardise the performance of tasks by the judicial authorities and services or institutions responsible for the protection of public order, citizens' security or prosecution of perpetrators of crime or fiscal crime;
- making information available could pose threat to the security of the state or the public order;
- the State of residence of the foreign FIU submitting the request for information does not guarantee an adequate level of protection of personal data.

274. The GIFI may also exchange information with the competent authorities of other countries, foreign institutions and international organisations dealing with counteracting money laundering and financing of terrorism (including EUROPOL) and the European supervision authorities. To this end, it may conclude agreements specifying the mode and technical conditions for the exchange of information.

275. When initiating other measures to counteract money laundering and financing of terrorism, the GIFI may also conclude agreements with private sector entities other than obligated institutions in order to collect additional information relevant for the performance of its tasks.

276. An important supporting role is played by the Financial Security Committee (FSC), which acts as an opinion-forming and advisory body to the GIFI in the area of money laundering and financing of terrorism. Among other things, the FSC issues opinions on national assessments of the risk of money laundering and financing of terrorism and on a strategy containing an action plan aimed at reducing the risk related to these crimes, issues recommendations and opinions on the application of specific restrictive measures against a person or entity as well as analyses and evaluates legal solutions in the field of counteracting money laundering and financing of terrorism.

277. The Committee is composed of representatives of the minister competent for internal affairs, the Minister of Justice, the minister competent for foreign affairs, the Minister of National Defence, the minister competent for economy, the minister competent for public finance, the minister competent for computerisation, the minister - member of the Council of Ministers competent for coordinating the activities of special services, the Chair of the Polish Financial Supervision Authority, the President of the National Bank of Poland, Commander-in-Chief of the Police, Commander-in-Chief of the Military Police, Commander-in-Chief of the Border Guard, National Prosecutor, Head of the Internal Security Agency, Head of the Central Anti-Corruption Bureau, Head of the Intelligence Agency, Head of the Military Intelligence Service, Head of the Military Counterintelligence Service, Head of the KAS, Head of the National Security Bureau. Due to the scope of the envisaged tasks, the Committee members, apart from their knowledge of counteracting money laundering and financing terrorism, must additionally meet the requirements set out in the regulations on the protection of classified information in the scope of access to classified information with a classification not lower than "secret".

4.3.2. Obligated institutions

278. In accordance with the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, obligated institutions include:

1) national banks, branches of foreign banks, branches of credit institutions, financial institutions established in the territory of the Republic of Poland and branches of financial

institutions other than established in the territory of the Republic of Poland, within the meaning of the *Act of 29 August 1997 – Banking Law*;

2) cooperative savings and credit unions, and the National Cooperative Savings and Credit Union, within the meaning of the *Act of 5 November 2009 on Cooperative Savings and Credit Unions*;

3) domestic payment institutions, domestic electronic money institutions, branches of European Union payment institutions, branches of EU and foreign electronic money institutions, small payment institutions, offices of payment services and clearing agents within the meaning of the *Act of 19 August 2011 on payment services*;

4) investment firms, custodian banks within the meaning of *the Act of 29 July 2005 on trading in financial instruments* and branches of foreign investment firms within the meaning of that Act, operating in the territory of the Republic of Poland;

5) foreign legal entities pursuing brokerage activities in the territory of the Republic of Poland, including those conducting such activity in the form of a branch and commodity brokerage houses within the meaning of the *Act of 26 October 2000 on commodity exchanges* and commercial companies referred to in Article 50a of that Act;

6) companies operating a regulated market - in the scope they operate an auction platform referred to in Article 3(10a) of the *Act of 29 July 2005 on trading in financial instruments*;

7) investment funds, alternative investment funds, investment fund management companies, AIC management companies, branches of management companies and branches of management companies from the EU located in the territory of the Republic of Poland, within the meaning of the *Act of 27 May 2004 on investment funds and alternative investment fund management*;

8) insurance companies conducting the activity referred to in section I of the Annex to the *Act of 11 September 2015 on insurance and reinsurance activity*, including domestic insurance companies, main branches of foreign insurance companies with the registered office in a country which is not a Member State of the European Union and branches of foreign insurance companies with the registered office in another Member State of the European Union;

9) insurance intermediaries performing insurance intermediation activities within the scope of insurance listed in section I of the Annex to the *Act of 11 September 2015 on insurance and reinsurance activity* and branches of foreign intermediaries performing such activities with the registered office in the territory of the Republic of Poland, excluding an insurance agent who:

   a) is an insurance agent performing insurance intermediation activities for the benefit of one insurance company within the scope of the same section in accordance with the Annex to the *Act of 11 September 2015 on insurance and reinsurance activity*,

   b) does not collect insurance premiums from the customer or from the insurance company for the amounts due to the customer;

10) Krajowy Depozyt Papierów Wartościowych S.A. (National Depository of Securities) and the company to which Krajowy Depozyt Papierów Wartościowych S.A. delegated the performance of activities in the scope referred to in Article 48(1)(1) of the Act of 29 July

2005 on trading in financial instruments, in the scope they operate securities accounts or omnibus accounts;

11) entrepreneurs conducting bureaux de change activities within the meaning of the *Act of 27 July 2002 - Foreign exchange law,* other entrepreneurs providing the service of currency exchange or the service of intermediation in currency exchange who are not other obligated institutions and branches of foreign entrepreneurs carrying out such activity in the territory of the Republic of Poland;
12) entities pursuing economic activity consisting in providing services in the scope of:
    a) exchange between virtual currencies and means of payment,
    b) exchange between virtual currencies,
    c) intermediation in the exchange referred to in subparagraph a or b, or
    d) operating accounts referred to in paragraph 2(17)(e) of the *Act 1 March 2018 on counteracting money laundering and financing of terrorism*;
13) notaries in the scope of activities performed in the form of a notarial deed, comprising:
    a) transfer of the ownership of an asset, including sale, exchange or donation of movable property or real estate,
    b) concluding an agreement on inheritance division, dissolution of co-ownership, life annuity, rent in exchange for the transfer of the ownership of an real estate and on distribution of jointly-held assets,
    c) assignment of the cooperative ownership title, title to premises, perpetual usufruct title and alleged promise of a separate ownership of premises,
    d) in-kind contribution following a company establishment,
    e) concluding the agreement documenting the contribution or increase of contributions to the company or increase of the share capital,
    f) transformation or merger of companies,
    g) disposal of an enterprise,
    h) disposal of shares in the company;
14) advocates, legal advisers, foreign lawyers, tax advisers to the extent they provide legal assistance or tax advisory activities to customers, in relation to:
    a) purchase or sale of a real estate, an enterprise or an organised part of an enterprise,
    b) management of cash, financial instruments or other customer's assets,
    c) concluding the agreement for maintaining a bank account, a securities account or performing activities related to maintaining of those accounts,
    d) in-kind contribution to a capital company or increase of the share capital of a capital company,
    e) creating, operating or managing capital companies or trusts

    - excluding legal advisers and foreign lawyers practising their profession under their employment relationship or service in offices providing services to public administration authorities, other government and local government units and entities other than companies referred to in Article 8(1)(1)-(3) of the *Act of 6 July 1982 on legal advisers* (Journal of Laws of 2018 item 2115 as amended) and legal advisers performing their profession under their employment relationship in entities other than referred to in Article 4(1)(1) and (3) of the *Act of 5 July 1996 on tax advisory services* (Journal of Laws of 2019 item 283 as amended);

15) tax advisers in the scope of tax advisory services other than specified in subparagraph 14 and statutory auditors;

16) entrepreneurs within the meaning of the *Act of 6 March 2018 - Entrepreneur law,* other than other obligated institutions, providing services consisting in:
   a) establishing a legal person or an organisational unit without legal personality,
   b) fulfilling a function of a member of the management board or enabling other person to fulfil this function or a similar function in a legal person or an organisational unit without legal personality,
   c) providing a registered office, address of establishment or address for correspondence and other related services to a legal person or an organisational unit without legal personality,
   d) acting or enabling other person to act as a trustee established by means of a legal act,
   e) acting or enabling other person to act as a person exercising its rights arising from stocks or shares to the benefit of an entity other than a company listed on the regulated market subject to the requirements related to information disclosure in compliance with the European Union law or subject to equivalent international standards;

17) entities pursuing activities in the scope of providing bookkeeping services;

18) intermediaries in real estate trading;

19) postal operators within the meaning of the *Act of 23 November 2012 - Postal Law* (Journal of Laws of 2018 item 2188 as amended);

20) entities carrying out activity in the scope of games of chance, betting, card games and games on gaming machines, within the meaning of the *Act of 19 November 2009 - Gambling law* (Journal

21) foundations established pursuant to the *Act of 6 April 1984 on Foundations* (Journal of Laws of 2016, item 1491) to the extent they accept or make cash payments of the total value equal to or exceeding the equivalent of 10.000 EUR, regardless of whether the payment is performed as a single operation or as several operations which seem linked with each other;

22) associations with legal personality established pursuant to the *Act of 7 April 1989 - Law of associations* (Journal of Laws of 2016, item 713) to the extent they accept or make cash payments of the total value equal to or exceeding the equivalent of EUR 10,000 regardless of whether the payment is performed as a single operation or as several operations which seem linked with each other;

23) entrepreneurs, within the meaning of the *Act of 6 March 2018 - Entrepreneur law*, to the extent they accept or make cash payments for goods of the total value equal to or exceeding the equivalent of EUR 10,000 regardless of whether the payment is performed as a single operation or as several operations which seem linked with each other;

24) entrepreneurs, within the meaning of the *Act of 6 March 2018 - Entrepreneur law* to the extent they carry out activity consisting in making safe deposit boxes available and foreign entrepreneurs carrying out such activity in the territory of the Republic of Poland;

25) credit granting institutions within the meaning of the *Act of 12 May 2011 on consumer credit*.

279. The Act imposes the obligation on obligated institutions to apply customer due diligence measures towards their customers. The scope of customer due diligence measures applied takes into account the identified money laundering and financing of terrorism risk related to business relationship or an occasional transaction as well as its assessment.

280. The obligated institutions shall apply the customer due diligence measures in the case of:

1) establishing business relations;
2) performing an occasional transaction with the value equivalent to EUR 15,000 or more, irrespective of whether the transaction is conducted as a single operation or as several operations which seem to be linked to each other or which constitutes a cash transfer referred to in Article 3(9) of *Regulation (EU) 2015/847 of the European Parliament and of the Council* for the amount exceeding the equivalent of EUR 1000;
3) carrying out a cash occasional transaction of the equivalent of EUR 10,000 or more, regardless of whether the transaction is carried out as a single operation or several operations which seem to be linked to each other in the case of the aforementioned entrepreneurs within the meaning of *the Act of 6 March 2018 - Entrepreneur law*, accepting or paying for goods in cash with a value equal to or exceeding the equivalent of EUR,10 000;
4) betting a stake and collecting prizes with the value equivalent to EUR 2,000 or higher, irrespective of whether the transaction is conducted as a single operation or as several operations which seem to be linked - in the case of entities pursuing activity in the scope of games of chance, betting, card games and games on gaming machines;
5) suspicion of money laundering or financing of terrorism;
6) doubts regarding the authenticity or completeness of customer identification data obtained so far.

281. The obligated institutions may apply:

- simplified customer due diligence measures in cases where a risk assessment has confirmed a lower risk of money laundering or financing of terrorism;
- enhanced customer due diligence measures in cases of business relations or occasional transactions involving a higher risk of money laundering or financing of terrorism, as well as, inter alia, towards customers originating in or established in a high-risk third country.

282. In order to mitigate the risk of money laundering and terrorism financing and to provide for the proper management of identified risk of money laundering or financing of terrorism, the obligated institutions shall be bound to introduce an internal procedure on counteracting money laundering and financing of terrorism and to appoint a person at a management level as responsible for the implementation of the obligations specified in the Act.

283. Moreover, the obligated institutions shall be bound to develop and implement an internal procedure of anonymous reporting (whistleblowing) of real or potential infringements of the provisions in the scope of counteracting money laundering and financing of terrorism by employees or other persons performing activities for the obligated institution.

284. The Act imposes an obligation to provide the GIFI with information, in particular on the so-called above-threshold transactions, i.e.

1) The following transactions by all obligated institutions except for entrepreneurs pursuing bureaux de change activities, other entrepreneurs providing foreign exchange services or foreign exchange intermediation services (which are not other obligated institutions), branches of foreign entrepreneurs conducting such activities in the territory of the Republic of Poland, notaries, advocates, legal advisers, foreign lawyers and tax advisers:
    - accepted payment or executed disbursement of cash exceeding the equivalent of EUR 15,000;
    - performed transfer of funds[90] of a value exceeding EUR 15,000 (also in the case of a transfer originating from outside the Republic of Poland to a recipient whose payment service provider is an obligated institution), with certain exceptions specified in its provisions.
2) Executed purchase or sale transaction of foreign currency with the equivalent exceeding EUR 15,000, or intermediation in executing such transaction by all obligated institutions.
3) Notarial acts with the equivalent exceeding EUR 15,000 carried out by notaries (but only in respect of notarial acts for which they are obligated institutions).

285. An obligation was also imposed on obligated institutions to notify the GIFI of circumstances that may indicate a suspicion of money laundering or financing of terrorism crime, without delay, but not later than within 2 business days from the date of confirming the circumstances.

286. Moreover, they were obligated to notify immediately in the case of acquiring a justified suspicion that the transaction or property values may be related to money laundering or financing of terrorism. In such a case, until the receipt of a request to block the account or suspend the transaction or an appropriate exemption, however, not longer than for 24 hours, counted from the moment of confirming the receipt of the notification, the obligated institution shall not execute the above transactions or other transactions debiting the account on which suspicious property values were accumulated.

287. At the request of the GIFI (issued also independently of the notification submitted in the above manner), obligated institutions shall block accounts or suspend transactions for the period specified in the request. If they result from the notification provided by an obligated institution, of a justified suspicion that the transaction or property values may be related to money laundering or financing of terrorism, the period of blocking the account or suspending the transaction imposed by the GIFI shall not exceed 96 hours, counting from the date and time indicated in the confirmation of receipt of the notification. Otherwise, the period of account blocking or suspension of a transaction imposed by the GIFI shall not exceed 96 hours, counting from the moment of receiving the demand by the obligated institution.

288. Obligated institutions shall also block accounts or suspend transactions in connection with a decision of the public prosecutor issued in this respect pursuant to the provisions of this Act.

[90] Within the meaning of Regulation *of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006* (OJ L 141, 05.06.2015, p. 1), i.e. relating to transactions executed through payment service providers.

In such a case, blocking of the account or suspension of the transaction shall not last longer than 6 months (counting from the date of receiving the notification from the GIFI - in case it is a follow-up of the earlier blocking of the account or suspension of the transaction imposed by the GIFI).

289. The GIFI may exempt the obligated institution from the obligation to refrain from performing the transaction according to the procedure described above, in the case if the available information does not provide grounds to notify the prosecutor of suspected crime of money laundering or financing of terrorism or in the case of recognising that the transaction suspension or account blocking could jeopardise the performance of tasks by the judicial authorities and services or institutions responsible for the protection of public order, citizens' security or prosecution of perpetrators of crime or fiscal crime and judiciary authorities.

290. At the request of the GIFI, the obligated institutions shall immediately transfer or make available information or documents necessary for the performance of its tasks, including with regard to: clients, executed transactions, type, amount and place of storage of assets, application of a customer due diligence measure, IP addresses from which the connection with the ICT system of the obligated institution was made and the time of connections with this system.

291. Additionally, the GIFI may require an obligated institution to monitor the indicated business relations or occasional transactions. In its request, it shall specify the scope of information obtained within the framework of the monitoring as well as the time of obtaining it (i.e. conducting monitoring) as well as the date and form of providing or making available information or documents to the GIFI .

292. In order to counteract terrorism and financing of terrorism, the obligated institutions shall apply the specific restrictive measures set out in Article 117(1) of the Act against persons and entities indicated in the lists referred to in United Nations Security Council Resolutions, issued under Chapter VII of the Charter of the United Nations, concerning threats to international peace and security caused by terrorist acts, in particular the lists referred to in paragraph 3 of *United Nations Security Council Resolution 2253 (2015)* or paragraph 1 of *United Nations Security Council Resolution 1988 (2011)* as well as those designated in the list referred to in Article 120(1) of the Act.

293. The obligated institutions are controlled by the GIFI with respect to their performance of the obligations in the area of counteracting money laundering and financing of terrorism. They shall also carry out checks within their jurisdiction in accordance with the rules laid down in separate provisions:

- the President of the NBP (in relation to entities carrying out bureaux de change activity within the meaning of the *Act of 27 July 2002 - Foreign exchange law*);
- KNF (PFSA) (in relation to institutions supervised by it);
- National Cooperative Savings and Credit Union (in relation to cooperative savings and credit unions);
- presidents of courts of appeals (in relation to notaries public);
- heads of customs and tax control offices (with respect to all obligated institutions).

294. Moreover, under the principles set out in *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, such control may be carried out by governors of the

province or governors of the district - with regard to associations as well as by ministers or governors of the district - with regard to foundations.

295. An obligated institution which violates the obligations specified in the Act and in the provisions of Regulation 2015/847 shall be subject to an administrative penalty.

296. In accordance with the Act, administrative penalties include:

- publication of information on the obligated institution and the scope of violation of the provisions of the Act by this institution in the Public Information Bulletin on the website of the office providing services to the minister competent for public finance;
- the order to cease undertaking specific activities by the obligated institution;
- ban on the performance of regulated activity for up to three years and striking off from the register of regulated activity;
- prohibition of holding a managerial position by a person responsible for the violation of the provisions of the Act by the obligated institution over a period of maximum one year;
- financial penalty.

4.3.3. Cooperating units

297. In accordance with the Act, cooperating units shall mean: government, local government authorities and other state organisational units as well as the National Bank of Poland (NBP), the Polish Financial Supervision Authority (KNF (PFSA)) and the Supreme Audit Office (NIK);

298. On request of the GIFI, units cooperating within the scope of their statutory competence shall provide or make available any information or documents held. In order to provide the aforementioned information or documents, the GIFI may conclude an agreement with a cooperating unit, defining technical conditions of providing information or documents or making them available.

299. Moreover, the cooperating units shall immediately inform the GIFI of any suspicion involving committing money laundering and financing of terrorism and develop the instructions concerning the procedure in such cases. If the above mentioned notifications provided the grounds for notifying the prosecutor's office about a suspicion of committing one of the above mentioned crimes by the GIFI, the GIFI - not later than within 30 business days - shall inform the cooperating unit which provided the information constituting the basis for the notification. Additionally, the GIFI, also not later than within 30 days, shall inform the Internal Security Agency, the Central Anti-Corruption Bureau, the Police, the Military Police and the Border Guards about circumstances indicating a connection between the information contained in the aforementioned notifications and the information received from obligated institutions concerning:

- circumstances which may indicate the suspicion of committing an offence of money laundering or financing of terrorism;
- cases of raising a reasonable suspicion that the specific transaction or the specific property values may be related to money laundering or financing of terrorism;

- notification of the competent prosecutor of any case of a reasonable suspicion that the property values subject to the transaction or collected on the account originate from a crime other than the crime of money laundering or financing of terrorism or a fiscal crime, or are associated with a crime other than the crime of money laundering or financing of terrorism or a fiscal crime.

300. The Border Guard bodies and the heads of customs and tax control offices shall provide the GIFI with the information referred to in Article 5 of *Regulation (EC) No 1889/2005 of the European Parliament and the Council of 26 October 2005 on controls of cash entering or leaving the Community* (OJ L 309, 25.11.2005, p. 9) and with the information contained in the declaration referred to in the regulations issued under Article 21 of the *Act of 27 July 2002 - Foreign exchange law*. This information is provided by the 14th day of the month following the month in which the import of cash in the territory of the Republic of Poland, or export of funds from the territory of the Republic of Poland, has been performed. The bodies of the Border Guard provide information through the Chief Commander of the Border Guard.

301. Moreover, the GIFI shall make available the information in his possession on a written and justified request of:

1) Chief Commander of the Police;
2) Commander of the Central Bureau of Investigation of the Police;
3) Chief Commander of the Military Police;
4) Chief Commander of the Border Guard;
5) Head of the Internal Security Agency;
6) Head of Intelligence Agency;
7) Head of the Military Counterintelligence Service;
8) Head of the Military Intelligence Service;
9) Head of the Central Anti-Corruption Bureau;
10) Internal Supervision Inspector;
11) Commander of the Office for Internal Affairs of the Police;
12) Commander of the Office for Internal Affairs of the Border Guard;

- or persons authorised by them, in the scope of their statutory duties.

302. The GIFI shall also make available the information in his possession on a written and justified request of:

1) President of the Polish Financial Supervision Authority (PFSA) – in the scope of oversight exercised by the Polish Financial Supervision Authority pursuant to the *Act of 21 July 2006 on the financial market oversight*;
2) President of the Supreme Audit Office (NIK) – to the extent necessary to perform audit proceedings defined in the *Act of 23 December 1994 on the Supreme Audit Office*;
3) the national administrator referred to in Article 3(22) of Commission Regulation (EU) No 389/2013 of 2 May 2013 establishing a Union Registry pursuant to *Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No*

406/2009/EC of the European Parliament and of the Council and repealing Commission Regulations (EU) No 920/2010 and No 193/2011 (OJ L 122, 03.05.2013, p. 1) - within the scope of its competence;

4) the minister competent for foreign affairs – in the scope of its statutory competence in connection with the application of specific restrictive measures;

5) the minister competent for public finance – in connection with the request referred to in Article 11(2) of the *Gambling Law of 19 November 2009*.

303. The GIFI shall make available the information in his possession on a written and justified request of the Head of the KAS, director of the Revenue Administration Regional Office or Head of the Customs and Tax Control Office - in the scope of their statutory duties.

304. The GIFI, in particularly justified cases, may refuse to provide access to the information held by it to the above-mentioned entities, where such access could:

- negatively affect the process of analysing by the GIFI of information related to assets in relation to which a suspicion has been acquired that they may be associated with the crime of money laundering or financing of terrorism;
- expose a natural or legal person to a disproportionate damage.

305. In the event of suspecting that an offence or fiscal offence other than money laundering or financing of terrorism is being committed, the GIFI transfers the information justifying such suspicion to the competent authorities (i.e. the aforementioned law enforcement agencies, special services and the Head of the KAS) in order to undertake activities resulting from their statutory tasks. Additionally, in the case of a justified suspicion of a breach of regulations related to the functioning of the financial market, the GIFI provides information justifying this suspicion to the Polish Financial Supervision Authority (KNF (PFSA)). In the aforementioned situations, the cooperating units send feedback on the manner of using the received information within 90 days from the date of its receipt.

306. With regard to the fulfilment of statutory obligations by prosecutors, it should be indicated that the Act imposes an obligation on prosecutors to inform the GIFI about the issuance of a decision on:

- blocking the account or suspending the transaction;
- initiation of proceedings;
- presentation of charges;
- filing an indictment,

in cases of money laundering or financing of terrorism offences. The submission of the aforementioned information shall take place immediately, however, not later than within 7 days following the day of performing the activity of acquiring information. The information shall indicate, in particular, the circumstances related to committing the offence, including the indication of available identification data related to natural persons, legal persons and units without legal personality and the file reference number. The GIFI immediately informs the prosecutor about the information related to the above mentioned information.

307. A statutory obligation was also imposed on prosecutors to inform the GIFI, within 30 days (after receiving a notification from GIFI on suspicion that an offence referred to in Article 299 or 165a of the kk has been committed), about:

- issuing the decision on account blocking or transaction suspension;
- suspension of the proceedings;
- resumption of suspended proceedings;
- issuing the decision on the presentation of charges of criminal offence.

4.4. PERSONAL DATA PROTECTION

308. The information made available to the GIFI pursuant to the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* shall not be subject to the provisions limiting the disclosure of information or data covered by secrecy, except for classified information within the meaning of the provisions on the protection of classified information.

309. In fulfilling its tasks, the GIFI may collect and use necessary information containing personal data and process them within the meaning of the provisions on personal data protection (also without the knowledge and consent of the data subject), create collections of personal data and process information covered by telecommunications secrecy within the meaning of the provisions of *the Act of 16 July 2004. - Telecommunications law* (Journal of Laws of 2018 item 1954 as amended), i.e. related to IP addresses from which the connection of the obligated institution with the ICT system took place and times of connections with this system. However, in the case of data referred to in Article 14 of *the Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime* (Journal of Laws of 2019, item 125), the GIFI collects and processes them only when it is actually necessary due to the scope of tasks or activities performed.

310. The GIFI shall process financial information over a period in which such information is necessary for the execution of its statutory duties. The GIFI shall verify the need of continued processing of collected information at least once per 5 years. Information that is not necessary for the performance of statutory tasks shall be promptly deleted by the GIFI.

311. The GIFI shall provide, exclusively on request of the court or the prosecutor, when necessary in the course of conducted proceedings, personal data of:

1) natural persons making notifications on behalf of obligated institutions concerning:
    - circumstances which may indicate the suspicion of committing an offence of money laundering or financing of terrorism, or
    - cases of raising a reasonable suspicion that the specific transaction or the specific property values may be related to money laundering or financing of terrorism;
2) persons reporting the suspicion of money laundering or financing of terrorism within the internal structures of the obligated institutions,
3) persons reporting breaches of the regulations in the scope of counteracting money laundering and financing of terrorism;

4) employees of the Financial Information Department dealing with:

- analysing information related to property values, in relation to which the GIFI has become reasonably suspicious that it is associated with the crime of money laundering or financing of terrorism;
- carrying out of the procedure of transaction suspension or account blocking;
- requesting the submission of information on transactions and disclosure thereof;
- submission of information and documentation justifying the suspicion concerning the commitment of a crime to authorised bodies;
- exchange of information with cooperating units.

312. The above personal data, provided to the prosecutor or the court, cannot be made available to other entities or persons, with the exception of the persons referred to in:

- Article 156 § 1 of *the Code of Criminal Procedure*, i.e: in the course of legal proceedings - to parties, defence counsels, agents and statutory representatives and other persons with the consent of the President of the Court (with the possibility of making transcripts or copies of the case file), including by means of an ICT system, "... if technical considerations do not prevent this";
- article 156 § 5 of *the Code of Criminal Procedure*, i.e.: in the course of preparatory proceedings, "if there is no need to secure the proper course of proceedings or protection of an important state interest" - to parties, defence counsels, attorneys and statutory representatives as well as in exceptional cases, with the consent of the prosecutor, other persons (enabling making transcripts or copies of proceedings files and issuing certified copies or copies against payment), also in electronic form;
- Article 321 § 1 of *the Code of Criminal Procedure* (in the course of an investigation, if there are grounds for its closure - to a suspect or his/her defence counsel at their request, also in electronic form).

313. Any information collected and made available by the GIFI in accordance with the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* is covered by financial information secrecy. The GIFI makes it available only on the basis of the provisions of this Act (in the case of classified information within the meaning of the provisions on the protection of classified information, it is also made available in accordance with these provisions). Persons acting as financial information authorities, employees of the Financial Information Department of the Ministry of Finance as well as persons performing activities for this unit on the basis other than the employment relationship are obliged to maintain financial information secrecy. This obligation also exists after the termination of the function of a financial information authority, employment in the above mentioned unit or performance of activities for its benefit on the basis other than the employment relationship.

314. The aforementioned obligation to maintain the confidentiality of financial information shall also cover persons fulfilling the function of bodies authorised to acquire information pursuant to the procedure provided in the Act as well as employees, officers or persons performing activities in favour of those bodies. Although these bodies, their employees and officers performing activities in their favour may share information concerning the fact of

providing or acquiring information pursuant to the procedure foreseen in the Act, if this is necessary to ensure the accuracy of tasks executed by them.

315. In 2018, the Data Protection Officer was appointed at the GIFI in accordance with the provisions of *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.* (OJ L L 119, 4.5.2016, p. 1).

316. A separate control in the scope of obtaining by GIFI of information covered by telecommunications secrecy is exercised by the District Court in Warsaw.

5. MONEY LAUNDERING RISKS

5.1. RISKS RELATED TO PREDICATE OFFENCES

317. The offence of money laundering was criminalised in Article 299 of *the Penal Code* where the nature of this practice is defined. However, considering the risks associated with money laundering, especially in connection with risks arising from committing other offences, it is worth remembering that on 18 December 2013, Resolution no. I KZP 19/13 was adopted by the Criminal Chamber of the Supreme Court composed of seven judges, in which it was explicitly stated that the subject of crime under Article 299 of the Penal Code may include assets derived, directly or indirectly, from the act of committing a predicate offence for the purpose of money laundering may be also regarded as the perpetrator of money laundering. The Supreme Court gave this resolution a legally binding effect.

318. Article 299 of *the Penal Code*, penalizing money laundering, indicates that this practice may cover the "means of payment, financial instruments, securities, foreign exchange values, property rights or other movable property or real estate, stemming from the benefits related to committing of a prohibited act". In accordance with Article 115 § 1 of *the Penal Code*, "a prohibited act is the conduct that has the characteristics specified in the Penal Act". The concept of a prohibited act covers primarily criminal offences, i.e. offences prohibited by law under the pain of a penalty.

319. *Predicate offence* can therefore be any type of offence where the offender obtains property values by committing an offence. Predicate offences may include corruption offences, offences on the financial market (including stock exchange offences, insurance offences, conducting business without a licence), fiscal offences, illegal trade in narcotic drugs and psychotropic substances, human trafficking and smuggling of immigrants, illegal gambling, offences related to the infringement of copyright and industrial property rights, offences against property and against business transactions as well as other offences[91].

[91] In this respect, it is worth indicating that the offence specified in Article 165a of the kk is also the predicate offence for money laundering. This is compliant with FATF Recommendation No 5 (see International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated in October 2018, p. 11, available at:
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html).

Table no. 5 - Offences detected[92] by the Police and the Public Prosecutor's Office in completed preparatory proceedings in 2017 (extract from the GUS statistical yearbook of 2018)[93]

Type of offence	Number
offences against property	373,327
offences against general security and communication security	78,779
offences against the reliability of documents	60,409
offences against family and care	33,063
offences against the activities of state institutions and local self-government institutions	28,825
offences against freedom, freedom of conscience and religion	25,912
offences against life and health	20,660
offences against justice	18,859
offences against economic transactions	6,706
offences against money and securities trading	6,467
offences against public order	5,916
offences against sexual freedom and morality	5,575
offences against honour and physical integrity	3,422
offences under special laws:	
on counteracting drug addiction - the Act of 24 April 1997 (i.e., Journal of Laws of 2003 No. 24, item 198) and of 29 July 2005 (i.e. Journal of Laws of 2018 item 1030).	55,969
on copyright and the related rights (i.e. Journal of Laws of 2018 no. 90, item 1191)	14,031
on upbringing in sobriety and counteracting alcoholism (i.e. Journal of Laws of 2018 item 2137)	372
fiscal offences - kks	2,976
other	26,238

320. The largest number of offences recorded in 2017 were offences against property, within which in turn the largest group were frauds, i.e. offences committed pursuant to Article 286 and 287 of the kk (122,498) which accounted for approx. 16.0% of all identified offences. Crimes against the reliability of documents, i.e. crimes referred to in Articles 270-277 of the kk also constitute a considerable group.

321. However, the importance of individual categories of offences should not be linked solely with the number of offences found. From the point of view of counteracting money laundering, the specific character of individual offences related both to the purpose of committing them and to the impact on the level of common security as well as the sum of assets which were in the possession of criminals as a result of their committing, is of greater importance.

322. For example, one of the categories of offences in which the highest number of committed offences was recorded in 2017 were offences against common security and security in communications, i.e. the offences defined in Articles 163-180 of the kk (78,779). It should be noted, however, that the vast majority of them (ca. 70.2%) were prohibited acts related to driving a vehicle on the road by a person under the influence of alcohol or intoxicating agent, i.e. criminalised in Article 178a of the kk which do not have any impact on the level of money

[92] A detected offence is an event which has been confirmed as a criminal offence in a concluded investigation. The data do not include criminal acts committed by minors.
[93] Statistical Yearbook of the Republic of Poland 2018, GUS, 2018, p. 149-151, available at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/.

laundering risk. However, it cannot be denied that the offences referred to in Chapter XX of *the Penal Code*, which were included in the aforementioned category of crimes, are serious.

323. The detection and combating predicate offences and money laundering are often carried out in the context of combating organised crime. According to CBŚP data, in 2018, 8,030 persons (in 2017 - 7,113) operating in 880 (in 2017 - 858) organised crime groups, including 742 Polish groups (in 2017 - 735), 128 international groups (in 2017 - 113), 5 Russian-speaking groups and 5 groups composed of foreigners (the same numbers as in 2017), were covered by the Central Investigation Bureau of the Police within the framework of operational matters conducted by the Central Investigation Bureau of the Police[94] A considerable part of these groups dealt with drug crime, i.e. 374 (in 2017 - 336) and economic crime, i.e. 292 (in 2017 - 305). Some also carried out so-called multi-criminal activities, i.e. 92 groups (2017 - 81).

324. As in 2017, the activities of the CBŚP in 2018 were aimed at limiting the activity of criminal groups of economic nature acting to the detriment of the State Treasury and first of all at combating such predicate offences as VAT fraud and excise offences related to illegal production and smuggling of cigarettes and tobacco import.

325. Below, brief descriptions of selected types of predicate offences for money laundering, including the fiscal offences mentioned above, are presented.

5.1.1. Fiscal offences

General characteristics

326. The *Act of 10 September 1999 - Penal Fiscal Code* (Journal of Laws of 2018, item 1958, as amended), hereinafter referred to as the kks, penalises acts consisting in violation of prohibitions and orders specified in the tax, customs and foreign exchange law, as well as in *the Gambling Law of 19 November 2009*[95]. A fiscal offence is an act prohibited by the kks under the threat of a fine determined in daily rates, a penalty of restriction of liberty or a penalty of deprivation of liberty.

327. One of the most recognised fiscal offences is value added tax (VAT) fraud. In this area, the following criminal *modi operandi* are used in different configurations:

- intra-Community and export/intra-Community carousel fraud (a carousel fraud mechanism is based on a fictitious movement (circulation) of goods between EU Member States and the creation of apparent commercial transactions through the circulation of invoices and other documents describing fictitious economic events);
- “missing trader” fraud;
- pretending of intra-Community supplies or exports where an unrecorded sale within the territory of the country really occurred;
- fraud involving the so-called “straw men” issuing “empty” VAT invoices which do not reflect real economic events (with the “missing trader” involved);

[94] Report on the activities of the Central Investigation Bureau of the Police for 2018 (in statistical terms), CBŚP, Warsaw 2018, p. 2, available at: http://www.cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.
[95] On the subject of fiscal offences concerning illegal gambling see chapter. 5.1.6.

- abuse of customs procedure 4200[96].

328. Empty invoices are issued by both existing and established operators as well as by fictitious operators, i.e. those who do not exist or who only exist on paper and, in fact, do not pursue any business.

329. The purpose of VAT fraud is:

- extortion of an undue refund of the VAT difference;
- evasion of all tax liability or a part thereof without disclosing the whole economic activity or any part thereof.

330. One of the types of VAT fraud is fraud in international transactions. Its purpose is to extort an undue refund of VAT due to fictitious transactions with foreign entities. The results of detection and control activities conducted by the KAS authorities show that the perpetrators often use industries which have been classified for many years as high-risk due to tax irregularities, in particular in connection with trade in products subject to excise duty. Excise goods are often simultaneously the subject of offences related to VAT fraud and the failure to pay excise tax.

331. VAT fraud was most often prosecuted under Article 56 of the kks (concerning tax fraud) or under Article 62 of the kks (concerning the violation of accounting procedure).

Statistics

332. In 2016-2017, in the course of tax and customs and tax inspections, VAT losses related to carousel fraud were found in the total amount of PLN 21.7 billion, of which: in 2016 - PLN 14.2 billion, and in 2017 - PLN 7.5 billion[97]

333. On the other hand, in 2018, 3.1 thousand customs and tax inspections were completed, in which irregularities were established for the total amount of approx. PLN 11.3 billion. About 82.2% of this amount related to arrangements in the scope of VAT (i.e. approx. PLN 9.3 billion).

Table no. 6 - Selected statistical data on preparatory proceedings in penal tax cases conducted in the KAS in 2017-2018

Activity	**2018**	**2017**
Number of preparatory proceedings in penal fiscal cases:	66,920	97,305
including fiscal crime cases:	17,059	22,882
including fiscal offence cases:	49,861	74,423
Number of preparatory proceedings concluded with filing a bill of indictment with the court:	37,248	64,953

[96] Customs procedure 4200 refers to the exemption from value added tax of imports of goods dispatched or transported from a third territory or a third country to a Member State other than the country of termination of the dispatch or transport of the goods under the provisions of *Council Directive 2006/112/EC of 26 November 2006 on the common system of value added tax* (OJ L 347, 11.12.2006, p. 1).

[97] In the above period, the KAS authorities (and previously the tax, tax control and customs authorities) initiated a total of 7,138 preparatory proceedings in the field of VAT fraud, including 3,490 in 2017 and 3,648 in 2016. The tax reductions in the scope of the above mentioned tax resulting from committed prohibited acts amounted to approx. PLN 1.67 billion in 2017 and approx. PLN 3.62 million in 2016.

including for fiscal offence:	30,669	56,471
including for fiscal crime:	6,579	8,482
Number of preparatory proceedings concluded with filing an application to the court for permission to submit to liability on a voluntary basis:	7,594	8,550
including for fiscal offence:	3,637	4,182
including for fiscal crime:	3,957	4,368
Number of indictments approved by the Prosecutor:	852	1,723
including for fiscal offence:	28	59
including for fiscal crime:	824	1,664

334. In the framework of activities associated with combating organised crime related to illegal production and trade in excise goods, in 2016-2018, the CBŚP officers liquidated 57 cigarette factories (26 in 2016, 12 in 2017 and 19 in 2018) and revealed 88 places where tobacco slices were illegally produced (46 in 2016, 20 in 2017 and 22 in 2018). Moreover, the CBŚP secured property in connection with the above mentioned cases.

Table No. 7 - Statistical data of the CBŚP concerning the security measures in cases of illegal production and trade in excise goods in 2016-2018.

year	**PRODUCT**	cigarettes (pieces)	tobacco (kg)	alcohol (litres)
2016	CBŚP securing in the conducted cases	199,981,271	305,623	42,770
	Securing of property of other police units and other services in matters referred to them by the CBŚP	104,160,678	178,859	36,328
2017	CBŚP securing in the conducted cases	168,862,819	259,352	29,802
	Securing of property of other police units and other services in matters referred to them by the CBŚP	129,341,200	115,542	25,168
2018	CBŚP securing in the conducted cases	156,307,118	267,100	20,887
	Securing of property of other police units and other services in matters referred to them by the CBŚP	115,002,405	214,003	20,614

Examples of sanitized cases

Example no. 1.

In 2018, the CBŚP carried out many economic cases, such as the investigation of VAT fraud in fuel trade, where the value of losses to the detriment of the State Treasury is about PLN 700 million. The funds obtained in this way were laundered through transactions in bank accounts - simulated as legal business activity, acquisition of luxury goods such as real estate, expensive cars or jewellery and transferred across borders through companies established for this purpose in Cyprus and Switzerland. As a result of the work of police officers and prosecutors, property in bank accounts in the so-called tax havens was established, i.e. in the Principality of Liechtenstein (EUR 36 million) and Switzerland (CHF 14 million), in relation to which the prosecutor issued decisions on seizing the property. Currently, legal and procedural activities are in progress to cause the transfer of these funds to Poland. On the basis of the evidence gathered, 25 persons were charged. Property belonging to suspects was also seized for the total amount of over PLN 230 million, of which over PLN 184 million was secured in 2018.

Example no. 2.

The CBŚP conducts preparatory proceedings concerning the activity of Polish and foreign commercial law companies whose activity in the years 2017-2018 consisted, among others, in VAT extortion in connection with international and domestic trade in gas in the network *system. The resulting tax liability in the amount of over PLN 80 million was eliminated/compensated. Money laundering was found to occur through, among others, banking transactions carried out by a number of identified Polish and foreign companies. As a result of actions taken by officers and cooperation with the GIFI, e.g. through the use of blockades on bank accounts of companies benefiting from illegal activities, over PLN 87 million was seized.*

5.1.2. Corruption

General characteristics

335. In Polish law, corruption offences are regulated primarily in Article 228, Article 229, Article 230, Article 230a, Article 231, Article 250a, Article 296a and Article 302 of the Penal Code. A separate regulation is also provided for in the *Act of 25 June 2010 on Sport* (Journal of Laws of 2018 item 1263 as amended), where corruption related to sports competitions was criminalised.

336. Bribery is one of the most common predicate offences faced in practice, from which financial benefits subject to laundering originate. A subject of active bribery can be any person who gives or promises to give a bribe in exchange for the settlement of a matter of his/her interest in an office or institution by a person accepting a financial or personal benefit or its promise. A subject of passive bribery (merchantability) may be a public official or a person who is not a public official but acts as a public official, receiving (taking) a bribe.

337. A public official is a person referred to in Art. 115 § 13 of the kk, i.e:

- the President of the Republic of Poland;
- an MP, a senator, a councillor;
- Member of the European Parliament;
- a judge, a juror, a prosecutor, an officer of a financial body of preparatory proceedings or a superior body over a financial body of preparatory proceedings, a notary public, a bailiff, parole officer, a trustee, a court supervisor and a manager, a person adjudicating in disciplinary bodies acting pursuant to this Act;
- a person who is an employee of a government administration, other state authority or local government, unless he or she performs exclusively service activities and another person in the scope in which he or she is authorised to issue administrative decisions;
- a person who is an employee of a state control authority or a local government control authority, unless he or she performs exclusively service activities;
- a person occupying a managerial position in another state institution (i.e. heads of institutions, their deputies, heads of departments and divisions);
- an officer of a body appointed to protect public security (e.g. the Police, the ABW, the Border Guard) or an officer of the Prison Service;
- a person in active military service, with the exception of territorial military service provided at disposal;
- an employee of an international criminal court, unless he/she performs exclusively service activities.

338. Pursuant to Art. 115 § 19 of the Penal Code, a person fulfilling a public function is a public officer, a member of a self-government body, a person employed in an organisational unit which has public funds at its disposal, unless he/she performs exclusively service activities as well as another person whose rights and obligations in the scope of public activity are defined or recognised by the Act or by an international agreement binding on the Republic of Poland. Persons performing solely service activities are persons who do not exercise the substantive competence of a body, do not have the power to manage and take decisions in this respect, only facilitate the work of these bodies.

339. A proceeds are any good that can satisfy a specific need and its value can be expressed in money. It can be not only the increase in assets but also all beneficial agreements, e.g. a loan granted on favourable terms.

340. A personal benefit is a non-economic benefit that improves the situation of the person who receives it (e.g. promotion promise, decoration, vocational training).

Statistics

341. In 2016, 25,968 corruption offences were registered, including over 67% offences described in Article 271§ 3 of the kk.

Table no. 8 - CBA statistics concerning the number of identified corruption offences in 2016.

Legal qualification *(according to article)*	**Police**	**ABW**	**CBA**	**Prosecutor's office**	**SG**	**ŻW**	**Total**
Article 228 of kk	4,363	8	62	50	9	4	4,496
Article 229 of kk	1,789	4	53	36	69	0	1,951
Article 230 of kk	423	2	29	10	0	3	467
Article 230a of kk	171	3	11	8	0	1	194
Article 231 § 2 of kk	784	4	60	51	2	11	912
Article 250a of kk	15	0	13	0	0	0	28
Article 271 § 3 of kk	17,494	4	23	6	4	0	17,531
Article 296a of kk	134	0	7	0	0	0	141
Article 296b of kk	0	0	0	0	0	0	0
Article 305 of kk	221	1	18	4	0	2	246
Article 48 of Act *on sport*[98]	1	0	0	0	0	0	1
Article 54 of the Act on refunding[99]	1	0	0	0	0	0	1
Total	**25,396**	**26**	**276**	**165**	**84**	**21**	**25,968**

[98] *The Act of 25 June 2010 on Sport* (Journal of Laws of 2018 item 1263 as amended).
[99] *Act of 12 May 2011 on the refunding of medicines, foodstuffs for particular nutritional use and medical devices* (Journal of Laws of 2019 item 784 as amended).

342. According to data from the Police, the Police conducted 1,697 proceedings initiated in 2016 - the highest number among all services authorised. The ABW conducted 11 such proceedings, the CBA - 107, the SG - 65 and the ŻW - 32.

343. In 2017, 36,247 corruption offences were registered, i.e. by over 28% more than in the previous year. The most frequently recorded offence in 2017 was the certification of untruth in a document for the purpose of financial or personal gain.

Table no. 9 - CBA statistics concerning the number of identified corruption offences in 2017.

Legal qualification ***(according to article)***	**Police**	**ABW**	**CBA**	**Prosecutor's office**	**SG**	**ŻW**	**Total**
Article 228 of kk	5,162	2	91	153	54	6	5,468
Article 229 of kk	1,884	1	53	156	107	3	2,204
Article 230 of kk	709	1	38	25	3	3	779
Article 230a of kk	127	0	10	7	0	0	144
Article 231 § 2 of kk	2,013	4	88	115	9	16	2,245
Article 250a of kk	11	0	0	0	0	0	11
Article 271 § 3 of kk	24,753	7	30	28	7	4	24,829
Article 296a of kk	251	0	66	0	0	0	317
Article 296b of kk	0	0	0	0	0	0	0
Article 305 of kk	231	1	5	6	1	2	246
Article 46 of the *Act on Sport*[100]	2	0	0	1	0	0	3
Article 47 of the *Act on Sport*[101]	1	0	0	0	0	0	1
Total	**35,144**	**16**	**381**	**491**	**181**	**34**	**36,247**

344. In 2017, the largest number of preparatory proceedings in corruption cases was initiated by the Police - 1681, by the ABW - 10, by the CBA - 92, by the KAS - 2, by the SG - 70, by the ŻW - 49.

345. In 2018, the CBA instituted 189 preparatory proceedings (98 were conducted on own materials and 74 on materials entrusted to it by the prosecutor's office). In total, at that time the Bureau conducted 567 proceedings and completed 173 of them. As a result, 721 suspects were charged with 2,226 charges.[102]

Examples of sanitized cases

Example no. 1.

The preparatory proceedings concerned, among others, granting financial gains with the value of at least PLN 170 thousand in exchange for unlawful influence on decisions of the management board of a company with State Treasury shareholding and a promise to grant financial gains of at least PLN 1 million and to grant benefits of at least PLN 500 thousand in exchange for mediation in handling matters in state institutions. One of the cases mentioned above was to influence the decision of the Regional Conservator of Monuments in the Małopolskie Province to discontinue the proceedings concerning the registration of the building of the former Cracovia hotel in the register of monuments.

[100] *Act of 25 June 2010 on Sport*.
[101] *Act of 12 May 2011 on the refunding of medicines, foodstuffs for particular nutritional use and medical devices*
[102] Information on results of activity of the Central Anti-Corruption Bureau in 2018, CBA 2019, p. 8, available at: https://cba.gov.pl/pl/aktualnosci/4091,Informacja-o-wynikach-dzialalnosci-CBA-w-2018-roku.html.

The investigation concerning the invocation of influences in Grupa Azoty S.A., Grupa Lotos S.A., the Oil and Gas Institute - State Research Institute. In the course of the proceedings, the issue of invoking the influence in Grupa Azoty S.A. and undertaking to settle the issue in the form of a guarantee of delivery of raw materials to Grupa Azoty S.A. in exchange for property benefits in the form of an additional investment of PLN 40 million was examined. In addition, the investigation concerns invoking the influence in the Institute of Oil and Gas - State Research Institute and undertaking to settle the matter in the form of obtaining a certificate for a defined company, necessary to trade with Grupa Lotos SA, in exchange for a financial benefit of PLN 100 thousand.

Example no. 2.

The case of Marek C was heard before the District Court in B. (in connection with the conduct constituting an infringement of the provisions of the Act of 29 January 2004 - Public procurement law, with regard to the obligation to maintain impartiality and objectivity as well as equal treatment of all tender participants) who, in the years 2009-2011, acting as the head of the IT department of one of the tax offices, in the course of public procurement proceedings, accepted from Jarosław S. - Director of the Q. Company's Branch, a financial benefit of a total value of at least PLN 2,500. The accused was sentenced to one year of imprisonment and a fine of 100 daily rates of PLN 25 each.

Example no. 3.

The case of Arkadiusz Z. was heard before the District Court in B., who in 2013, in connection with the service of the head of commune and activities aimed at selling the real estate located in B. to the E. company, accepted a financial benefit of PLN 20,000 from Arkadiusz B. and Wojciech S. In the same proceedings Arkadiusz B. and Wojciech S. were accused of granting the financial gain to Arkadiusz Z.

The following penalties were imposed on the accused: Arkadiusz Z. 1 year imprisonment suspended for a trial period of 3 years, a fine of 150 daily rates, setting one rate at PLN 100 and a penal measure in the form of forfeiture to the State Treasury of a benefit derived from a crime in the amount of PLN 20,000. Arkadiusz B and Wojciech S. were sentenced to 1 year of imprisonment suspended for a trial period of 3 years and a fine of 100 daily rates, setting one rate at PLN 100.

5.1.3. Illicit trafficking in narcotic drugs and psychotropic substances

General characteristics

346. Money subject to laundering can also come from drug offences. In the *Act of 29 July 2005 on counteracting drug addiction* (Journal of 2019, item 852), the behaviour consisting in the marketing of narcotic drugs, psychotropic substances or poppy straw or participation in such marketing is penalised (Article 56). In addition, the use of a narcotic drug or a psychotropic substance, facilitation of or inducement to use such a drug or substance in order to obtain a financial gain shall be punishable (Article 59). Moreover, according to Article 61 of *the Act on counteracting drug addiction*, a person who, contrary to the provisions of the Law, Regulation

273/2004[103] or Regulation 111/2005[104], in order to manufacture a narcotic drug or a psychotropic substance illicitly, manufactures, processes, converts, imports, exports, imports, performs intra-Community purchase or intra-Community supply shall be also penalised. These types of offences are often committed within the framework of organised criminal structures, resulting in more severe criminal liability.

Statistics

Table No. 10 - Statistical data of the Police Headquarters concerning drugs discovered and seized in 2016-2017 as a result of their activity

Type of substance	Measurement Unit	2016	2017
Amphetamine	grams	511,195.7	617,892.7
Hashish	grams	10,371	25,732.9
Methamphetamine	grams	12,625.9	9,486.1
Heroin	grams	2,998.9	1,458.2
Cocaine	grams	17,033.1	12,251
Marijuana	grams	1,854,282.2	2,354,776.3
Mephedrone	grams	44,762.2	28,461.4
Ecstasy	pcs.	75,011	153,970
Cannabis (bush)	pcs.	86,810	91,714
LSD	pcs.	*no data*	*no data*
BMK	litre	*no data*	*no data*

Table No. 11 - Statistical data of the CBŚP concerning seized drugs, in cases conducted by the Bureau and referred to other units in the years 2016 - 2018[105]

Type of substance	Measurement Unit	2016	2017	2018
Amphetamine	grams	407,497	576,590	711,424
Hashish	grams	1,191,962	737,547	7,748,765
methamphetamine	grams	2,725	43,411	about 14,000
Heroin	grams	5,768	2,452	2,376
Cocaine	grams	36,656	67,031	23,750
Marijuana	grams	861,164	756,698	1,438,059
Ecstasy	pcs.	71,744	71,867	89,809
LSD	pcs.	170	11	780
BMK	litre	14	48	1580
Cannabis (bush)	pcs.	20,461	17,463	14,034

Table No. 12 - Statistical data of the Border Guard concerning drugs discovered and seized in 2016-2017 as a result of their activity

Type of substance	Measurement Unit	2016	2017
Hemp resin (hashish)	grams	14,591.74	499,609.55
Hemp herb (marijuana)	grams	82,941.22	2,863,381.10

---

[103] *Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors* (OJ L 47, 18.02.2004, p. 1).

[104] *Regulation (EC) No 111/2005 of the European Parliament and of the Council of 22 December 2004 laying down rules for the monitoring of trade between the Community and third countries in drug precursors* (OJ L 22, 26.01.2005, p. 1).

[105] In addition, during this time, the following substances were seized: MDMA - 350 kg (2017 - 69 kg), mephedrone - 1.5 kg (2017 - 7 kg), designer drugs - 153 kg and GBL - 1,075 litres.

Other pharmaceuticals (total)	pcs.	16,175	130,671
Ecstasy (pcs.)	(blister, vial)	3,166	40,748
Amphetamine	pcs.	33,471.72	5,897.77
methamphetamine	grams	2,641.03	659.59
Cannabis (bushes)	grams	1,276	448
Ecstasy	pcs.	291.13	86.87
Clonazepam	grams	-	82
4CMC - cathinon derivative	pcs.	-	43.24
Brown heroin	grams	21.48	35.39
Barbituran	grams	-	8.53
Cocaine	grams	145.96	14,024.25
White heroin	grams	0.68	-
Pseudoephedrine	grams	320,000	-
Hallucinogenic mushrooms	pcs.	1.8	-

347. Moreover, in the years 2016-2017, the regional police headquarters and the Warsaw Police Headquarters liquidated:

- 13 synthetic drug laboratories (6 in 2016 and 7 in 2017);
- 2 503 Cannabis plantations (1295 in 2016 and 1208 in 2017).

348. On the other hand, in 2016-2018, the CBSP liquidated:

- 53 synthetic drug laboratories (22 in 2018, 19 in 2017 and 12 in 2016);
- 202 professionally organised cannabis plantations (22 in 2018, 54 in 2017 and 108 in 2016).

349. In 2017, the illegal laboratory of designer drugs (4CMC), the so-called deadly designer drug popular among young people, was closed down. More than 120 kg of designer drugs and ingredients, from which huge quantities of the drug could be produced, were secured on site.

Examples of sanitized cases

Example no. 1.

The case of Maciej W. who in 2003-2008 took part in an organised criminal group aiming at committing crimes consisting in particular in importing into the EU and other European countries significant quantities of narcotic drugs in the form of cocaine in order to obtain financial gain, was heard before the Regional Court in Ł. In total, Maciej W. brought to Poland at least than 60,000 grams of this drug, transporting it in closed capsules, which he swallowed. The accused was sentenced to a total term of imprisonment of 5 years and additionally he was ordered to forfeit his financial benefit in the amount of PLN 240,000.

Example no. 2.

The case of Adria K., who in the period from January 2013 to May 2015 in Poland, Spain and other Member States of the European Union, as well as in the territory of Belarus and Ukraine, took part in an organised criminal group dealing with illicit transfer and distribution of significant amounts of narcotic drugs, and personally performed intra-Community acquisitions of significant amounts of narcotic drugs in the form of hashish, which he transported from Spain, across Poland to the territory of Ukraine and Belarus. The accused *was sentenced to the total of 2 years and 7 months imprisonment and the forfeiture of the equivalent of PLN 28,000 of the benefit gained by the accused from the crime and the forfeiture of a Kia Sportage passenger car was adjudicated.*

5.1.4. Human Trafficking and immigrant smuggling

General characteristics

350. In the Polish Penal Code, the crime of human trafficking is regulated in Article 189a of the kk which provides for a penalty of imprisonment for this act for not less than 3 years. It is also punishable to prepare to commit this act. In accordance with 115 § 22 of the kk, human trafficking is the recruitment, transports, delivery, transfer, storage or reception of a person by means of violence or threat of unlawful conduct, abduction, deception, misrepresentation or exploitation of an error or inability to properly understand an action taken, abuse of a relationship of dependence, exploitation of a critical position or a state of helplessness, granting or accepting a financial or personal benefit, or a promise thereof, to a person having custody or control over another person for the purpose of exploitation, even with his or her consent, in particular in prostitution, pornography or other forms of sexual exploitation, in forced labour or services, in begging, in slavery or in other forms of exploitation degrading human dignity, or for the purpose of obtaining cells, tissues or organs contrary to the provisions of law. If the conduct of the offender concerns a minor, it constitutes human trafficking even if the methods or means listed in subparagraph 1-6 of this provision have not been used.

351. Immigrant smuggling is penalised in Article 264 § 3 of the kk, where the organisation of crossing the border of the Republic of Poland by other persons is threatened with the penalty of deprivation of liberty.

352. In some countries, both offences are often the source of high profits for criminal groups involved in such activities. In Polish statistics, they occupy a marginal position.

Statistics

353. In 2016, the Police provided the prosecutor's office with materials on the basis of which the prosecutor's office initiated 31 preparatory proceedings, out of which:

- 4 were related to forced labour or services;
- 1 - for the procurement of cells, tissues or organs contrary to the provisions of the Act.

354. On the other hand, in 2017, 27 proceedings instituted on the basis of police materials concerned:

- 12 other forms of exploitation degrading human dignity (9 offers to sell an unborn child or an infant, 2 cases of exploitation in circumstances degrading human dignity and 1 forced marriage of convenience), including 4 in the form of preparation for a crime (3 cases of offers to sell a child and 1 forced marriage of convenience);
- 8 cases of exploitation in prostitution, pornography or other forms of sexual exploitation, including 1 in the form of preparation;
- 5 proceedings concerned forced labour or services, including 1 in the form of preparation;
- 2 - for begging, including 1 in the form of preparation.

Table no. 13 - Statistical data of the Police for the years 2016-2017 concerning detected potential victims of human trafficking on the basis of information from instituted proceedings

Country of origin of victims	**2016**	**2017**
Poland	**18** (in forced labour or services)	**8** (in forced labour or services)
	(in prostitution, pornography or other forms of sexual exploitation)	**18** (in prostitution, pornography or other forms of sexual exploitation)
	15 (other forms of exploitation degrading human dignity)	**7** (other forms of exploitation degrading human dignity)
	5 (in begging)	**4** (in begging)
Bulgaria	**1** (in prostitution, pornography or other forms of sexual exploitation)	**1** (in prostitution, pornography or other forms of sexual exploitation)
Macedonia	**7** (in forced labour or services)	
Serbia	**1** (in forced labour or services)	
Ukraine	**2** (in prostitution, pornography or other forms of sexual exploitation)	**2** (in prostitution, pornography or other forms of sexual exploitation)
	1 (other forms of exploitation degrading human dignity)	**1** (other forms of exploitation degrading human dignity)
Vietnam	**1** (in prostitution, pornography or other forms of sexual exploitation)	
Philippines		**1** (in prostitution, pornography or other forms of sexual exploitation)
unspecified	**1** (other forms of exploitation degrading human dignity)	

Table no. 14 - Statistical data of the Police for the years 2016-2017 concerning the aggrieved parties indicated in proceedings concluded under Article 189a of the kk.

Country of origin of victims	**2016**	**2017**
Poland	**6** (in prostitution, pornography or in other forms sexual exploitation)	**20** (in prostitution, pornography or in other forms sexual exploitation)
	1 (other forms of exploitation degrading human dignity)	**15** (other forms of exploitation degrading human dignity)
		46 (in forced labour or services)
Macedonia	**7** (in forced labour or services)	
Serbia	**1** (in forced labour or services)	
Ukraine		**2** (in prostitution, pornography or in other forms of sexual exploitation)
unspecified		**1** (other forms of exploitation degrading human dignity)

355. In addition, in 2017 the Border Guard initiated 14 new investigations (9 in the area of forced labour, 2 in the area of exploitation for prostitution, 2 in the area of exploitation for work and prostitution and 1 in other forms of exploitation).

Table no. 15 - Statistical data of the Border Guard for the years 2016-2017 concerning detected potential victims of human trafficking

Country of origin of victims	**2016**	**2017**
Belarus	-	2 (forced labour)
Bulgaria	1 (begging)	
Congo	1 (forced labour/sexual	

	exploitation)	
Nigeria	-	1 (prostitution)
Poland	2 (prostitution)	5 (prostitution)
Syria / Saudi Arabia	-	1 citizen Syria with its son, citizen of Saudi Arabia (domestic slavery)
Ukraine	99 (forced labour)	30 (forced labour)
Vietnam	1 (forced labour)	4 (forced labour)

Examples of sanitized cases

Example no. 1.

On 20 October 2015 the Regional Prosecutor's Office in Lublin filed an indictment with the Regional Court in Lublin against 11 accused persons in connection with the activities of an organised crime group dealing in human trafficking in the period from 2009 to 3 November 2014 on the territory of Poland and Finland. The procedure consisted in recruiting, transporting and delivering a large number of persons to Finland with a view to their exploitation in begging, after their prior misleading as to the nature of the work to be carried out. The accused persons misled them as to the nature of the work to be carried out in Finland and the income to be derived therefrom. By taking advantage of their critical position, they recruited them and then took part in their transport from the Republic of Poland to Finland in order to use them for activities that humiliate human dignity, consisting in collecting money to support allegedly ill health requiring treatment, disability or other difficult life situations and offering low-value wooden products in return, which was in fact begging. The accused persons created a permanent source of their income from this crime. In the course of the investigation, the total of 76 victims were revealed.

Example no. 2.

The District Prosecutor's Office in Wrocław filed an indictment against three men (citizens of Poland) accused of human trafficking, forcing them into prostitution and producing pornography involving minors. Between January 2014 and July 2015, the defendants recruited young boys pretending that they would be legally employed in Germany. Between a few and a dozen or so minor boys could be victims of the crime. So far, 9 victims have been identified, these were minor boys, one of whom was under the age of 15. The defendants earned more than 75,000 euros from this practice and the head of the group, a German citizen, is wanted by a warrant.

Example no. 3.

In 2015 The Appellate Prosecutor's Office in Gdańsk issued an indictment against two men accused of human trafficking and benefiting from prostitution performed by other persons. The Regional Court in Gdańsk, in a court judgement of 18 December 2015, sentenced the main offender (a Bulgarian citizen) to 3 years' imprisonment, the second defendant was sentenced to 10 months' imprisonment suspended for 2 years. The aggrieved women were Bulgarian citizens.

5.1.5. Offences against property and economic transactions

General characteristics

356. The source of financial gain may also be very common crimes against property, i.e. theft (Article 278 of the kk), theft with burglary (Article 279 of the kk), misappropriation (Article 284 of the kk), fraud (Article 286 of the kk) or against economic transactions, such as e.g.

causing damage in economic transactions (Article 296 of the kk) or credit fraud (Article 297 of the kk).

357. One of the most frequently committed crimes against property in Poland is the crime of fraud under Article 286 of the kk or credit fraud under Article 297 of the kk. This act is often committed in multi-person configurations, where the perpetrators' actions are aimed at making the criminal activity a permanent source of income.

358. This category of offences includes offence known as a pyramid scheme, based on the Ponzi scheme.

Examples of sanitized cases

Example no. 1.

The case is pending before the Regional Court in Ł. The accused Krystyna M. was accused of having acted jointly and in agreement with several dozen people in the years 2008-2011 and led several banking institutions to an unfavourable disposal of property in the total amount of several dozen thousand zlotys. Krystyna M. acted in the capacity of the President of the Management Board of B., a company dealing with construction and installation works. It issued certificates of income to friends and employees in order for them to obtain credits and loans and consequently, to gain a financial advantage for themselves. False certificates were presented to the lender, and the money obtained in this way was mostly received by the accused. Krystyna M. was sentenced for acts under Article 286 § 1 of the kk in conjunction with Article 297 § 1 of the kk in conjunction with Article 11 § 2 of the kk to the total penalty of 3 years' imprisonment; moreover, the court also imposed on her the obligation to repair the damage caused by the crime.

Example no. 2.

Ivo T. was accused of abusing his powers and failing to fulfil his obligations by acting, in order to obtain a financial advantage, as the Vice-President of the Management Board of a bank established in Ł., obliged to deal with the financial affairs of that bank and to properly secure its interests, and of taking decisions to grant investment loans to several economic entities, even though those entities did not have the creditworthiness or the required own contribution, and of doing so, in addition, without guaranteeing adequate security for the repayment of the loan. Since the remuneration of the accused depended on the number of loans granted, he acted not only to obtain a financial advantage for the borrower, but also for himself. By his actions, the accused person led the aforementioned bank to a damage of several million zlotys. He was sentenced for acts under Article 296 § 1, 2 and 3 of the kk to the total penalty of 2 years of imprisonment with conditional suspension of its execution for a period of 5 years of probation and obliged to partially repair the damage caused by the crime by paying the aggrieved party the amount of PLN 280 thousand.

Example no. 3.

One of the Branch Offices of the Department of Organised Crime and Corruption of the National Prosecutor's Office investigates the activities of an international criminal group which extorted funds held in bank accounts of business entities dealing in fuel products and electronics, using for this purpose enforcement proceedings initiated on the basis of fictitious enforcement titles in the form of counterfeit judgements of arbitration courts, in particular the *international arbitration court with its registered office in Warsaw and an arbitration court in one of the EU Member States.*

The vast majority of entities that were identified as companies affected by the activities of persons using arbitration court rulings are companies that in the years 2012-2014 participated in the extortion of value added tax (VAT) in Poland, in the mechanism of the so-called "carousel" fraud.

The amounts of tax depleted as a result of this practice, determined in the final decisions of tax authorities issued as a result of tax audits, were hedged by these authorities in the bank accounts of individual companies involved in the case for the purpose of settling tax liabilities.

The revealed criminal mechanism consisted in the creation of fictitious claims against companies subject to tax control, most often resulting from a promissory note issued by a taxpayer debtor on behalf of an entity established in another EU Member State.

The resulting claim was then secured by a registered pledge on a monetary claim (resulting, for example, from a promissory note allegedly issued by a debtor - a taxpayer of a promissory note for the benefit of a foreign entity). Pursuant to Article 20 of the Act on registered pledge and the pledge register (Journal of Laws of 2009, no. 67, item 569 as amended), the receivables secured by a registered pledge are subject to satisfying from the subject matter of the pledge with the priority over other receivables, unless the special provision provides otherwise.

After the entry in the pledge register, the obtained verdict of the arbitration court together with the decision of the common court to award the enforcement clause were then transferred to bailiffs as an enforcement title. In this way, the tax authorities were blocked from conducting enforcement proceedings and disposing of the previously secured amounts against due value added tax liabilities by launching court enforcement proceedings for alleged foreign creditors to whom promissory notes were issued.

The funds seized by the bailiffs in bank accounts were then transferred to the accounts of the companies belonging to the perpetrators, from where they were transferred to the bank accounts of subsequent recipients in other EU Member States.

***Example no. 4**[106]*

In cooperation with the District Prosecutor's Office in Warsaw and one of the national payment institutions, the GIFI thwarted an attempt to evacuate from Poland over PLN 44 million from the sale of "pseudo" crypto-currency, Dascoin. The notification sent by the GIFI to the prosecutor's office concerned a possibility of committing an offence under Article 286 of the Penal Code, i.e. leading to an unfavourable disposal of property by selling licences for the purchase of a number of products and services, including crypto-currency called Dascoin via the website www.netleaders.com. The findings of the GIFI and the prosecutor's office show that the model of remuneration of persons encouraged to join the Dascoin ecosystem was probably a pyramid-type promotional scheme, where the profit of the specific participant was directly dependent on the contributions of persons joining at a later date. In Poland, the Ponzi

[106] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, Warsaw 2019, p. 41.

scheme, the so-called "financial pyramid", is forbidden. The funds raised from the "shareholders" were then transferred abroad. The blocking of the last transfer worth over PLN 44 million made it possible to secure the funds of the fraudsters. Previously, the crypto-currency, Dascoin was declared a financial crime means by the North American Securities Administration Association[107].

5.1.6. Offences related to the infringement of copyright and industrial property rights

General characteristics

359. The financial benefits being subsequently the subject of a prohibited act specified in Article 299 of the kk may also originate from crime related to the infringement of copyright and industrial property rights.

360. Articles 115 - 122 of *the Act of 4 February 1994 on copyright and related rights* (Journal of Laws of 2018, item 1191, as amended) contain criminal provisions penalising infringements of copyright. Article 115(1) of the Act penalises the appropriation of copyright or misleading as to the copyright of another person's work or artistic performance. Distribution without the name or pseudonym of the author of another person's work in its original version or in the form of a study, artistic performance, phonogram, videogram or public broadcasting of such work, artistic performance, phonogram, videogram or broadcast shall also be punishable (Article 115(2)). Distribution without authorisation or contrary to the terms of another person's work in its original version or in the form of a development, artistic performance, phonogram, videogram or broadcast is also subject to criminal liability (Article 116(1)), similar to the recording or reproduction of such work for the purpose of distribution (Article 117(1)). Moreover, the Act also penalises activities consisting in purchasing, assisting in selling, accepting or assisting in hiding an object being the carrier of a work, artistic performance, phonogram or videogram disseminated or multiplied without a licence or against its conditions (Article 118(1)).

361. On the other hand, *Act of 30 June 2000 - Industrial property law* (Journal of Laws of 2017, item 776, as amended) provides for criminal liability for copyright authorship to oneself or misleading another person as to the copyright of another person's inventive design as well as for infringing the rights of the creator of an inventive design in another way (Article 303). An application for someone else's invention in order to obtain a patent is also penalised (Article 304). Under this Act, however, benefits subject to laundering under the offence stipulated in Article 299 of the kk are generated primarily from trade in goods bearing counterfeit trademarks. Pursuant to Article 305 of the Act, a person who designates goods with a counterfeit trademark or a registered trademark which he or she is not entitled to use for the purpose of marketing or who trades in goods bearing such trademarks, is subject to criminal liability (Article 305(1)). Stricter liability is imposed on perpetrators who make such activity a permanent source of income or commit this offence in relation to goods of significant value (Article 305(3)).

---

[107] Other cases of money laundering resulting from crimes related to the functioning of financial pyramids were presented, among others, in the *Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2016*, Warsaw 2017, p. 25.

Examples of sanitized cases

<u>Example no. 1.</u>

In the case pending before the Regional Court in Olsztyn. Piotr T. and Bartosz W. were accused of the fact that in the years 2013-2014, acting jointly and in agreement, they distributed without authorisation, via the Internet, third parties' original works in the form of several dozen types of computer games to the detriment of Microsoft Corporation as well as obtained other people's computer programs without the consent of authorised persons, acting to the detriment of Microsoft Corporation, Adobe Systems, ACD Systems and Cyberlink Software.

Piotr T. and Bartosz W. were sentenced under Article 116(1), (2) and (3) of the Act on copyright and related rights and Article 287 § 2 of the kk and other, to the total of 500 daily fine rates after setting a single rate of PLN 100 and an obligation to repair damage to the affected companies (Piotr T.) and 80 daily fine rates after setting a single rate of PLN 100 and an obligation to repair damage to the affected companies (Bartosz W.)

<u>Example no. 2.</u>

In the case pending before the Regional Court in Warsaw, in the years 2010-2011 Robert C. and Robert B. traded in medicinal products bearing counterfeit trademarks and medicinal products not admitted to trading, to the detriment of Pfizer INC, Bayer AG and Eli Lilly. Robert C. and Robert B. were convicted, inter alia, under Article 305(3) of the Act of 30 June 2000. - Industrial property law and Article 124 of the Act of 6 September 2001. - Pharmaceutical law for the following cumulative penalties:

a) Robert C. - for the penalty of 2 years of imprisonment suspended for a trial period of 3 years, a fine of 200 daily fine rates assuming the amount of one rate for 50 PLN, exemplary damages for the benefit of the affected companies in the amount of PLN 20,000 each. The accused was also ordered to forfeit the financial benefit derived from crime in the amount of PLN 1,275,161.25.

b) Robert B. - for the penalty of 1 year imprisonment suspended for a trial period of 3 years, a fine of 100 daily rates, assuming the amount of one rate of PLN 50, exemplary damages for the benefit of the affected companies in the amount of PLN 10 000 each. The accused was also ordered to forfeit the financial benefit derived from crime in the amount of PLN 100,000.

5.1.7. Other predicate offences

362. Apart from the aforementioned types of predicate offences, there are also other types of predicate offences, such as crime on the financial market (i.e. stock exchange crime, insurance crime, conducting business without a licence), offences related to illegal gambling or crime against the credibility of documents.

363. *The Act of 29 July 2005 on trading in financial instruments* regulates, inter alia, the rules, procedure and conditions for undertaking and conducting activities related to trading in financial instruments. It also contains criminal provisions providing for liability for offences consisting in: illegal activity in the field of trading in financial instruments (Article 178), illegal use of the markings referred to in Article 21(4a) and (5) (Article 178a), disclosure or use of professional or business secrecy (Article 179), disclosing or using inside information (Article 180), recommending or inducing to buy or sell financial instruments to which the inside

information relates (Article 182), manipulating financial instruments (Article 183(1)) or entering into an agreement aimed at manipulation (Article 183(2)). These offences can lead to obtaining financial gains subject to laundering.

364. The penal provisions are also contained in *the Act of 27 May 2004 on investment funds and management of alternative investment funds*. From the point of view of generating illegal profits subject to subsequent laundering, the crimes specified in Article 287 and 289 of the aforementioned Act are most important. The first of the aforementioned provisions provides for criminal liability for conducting, against the required permit or against the conditions specified in the aforementioned Act, the activity consisting in investing in securities, money market instruments or other property rights, assets of natural persons, legal persons or organisational units without legal personality, gathered by way of a proposal to conclude an agreement on participation in this undertaking (Article 287(1) of the aforementioned Act). On the other hand, in accordance with Article 289(1) of the aforementioned Act, criminal liability is imposed on a person who, being obliged to observe professional secrecy, discloses it or uses it contrary to its designation. Where the offender acts to obtain a financial or personal advantage, he or she is subject to more severe criminal liability.

365. The terms and conditions of making a public offer of securities, conducting a subscription or sale of these securities and applying for admission and introduction of securities or other financial instruments to trading on the regulated market are regulated by *the Act of 29 July 2005 on public offering, conditions governing the introduction of financial instruments to organised trading and public companies* (Journal of Laws of 2019, item 623)[108]. It also lays down the obligations of issuers of securities and other entities involved in trading in those securities or other financial instruments. Public offering of securities without meeting the conditions specified in the Act, i.e., for example, without the approval of the prospectus or the information memorandum, shall be subject to a fine of up to PLN 10 million, a penalty of imprisonment of up to 2 years, or both penalties jointly (Article 99). In addition, a person responsible for information contained in the prospectus or other information documents or for other information related to a public offering or admission or application for admission of securities or other financial instruments to trading on a regulated market, who provides false information or conceals true information that materially affects the content of such information, shall be liable to criminal prosecution. The motivation of the perpetrator for such crimes is usually the willingness to gain personal or financial advantage.

366. The KNF (PFSA) plays an important role in the disclosure of this type of offences. Pursuant to Article 6b(1) of *the Act of 21 July 2006 on the financial market oversight*, this authority shall make public information on the reports of the suspected commitment of the crime it has submitted defines in the following provisions:

- Article 215 and Article 216 of the *Act of 28 August 1997 on the organisation and operation of pension funds;*
- Article 171(1)-(3) of the *Act of 29 August 1997 – Banking Law*;

[108] From 21 July 2019, *Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market and repealing Directive 2003/71/EC* will apply in this respect (OJ L 168, 30.06.2017, p. 12), which significantly modifies the provisions of the aforementioned Act.

- Article 56a i Article 57 *of the Act of 26 October 2000 on commodity exchanges*;
- Article 430 of *the Act of 11 September 2015 on insurance and reinsurance activity* (before 1 January 2016 - Article 225 of *the Act on insurance activity*);
- Article 47 and Article 48 of *the Act of 22 May 2003 on insurance intermediation*;
- Article 50(1) and (2) of *the Act of 20 April 2004 on employee pension schemes;*
- Article 40 of *the Act of 20 April 2004 on individual pension accounts and individual accounts of pension security;*
- Article 287 and Articles 290-296 of *the Act of 27 May 2004 on investment funds and management of alternative investment funds;*
- Article 178 of *the Act of 29 July 2005 on trading of financial instruments;*
- Article 99 and Article 99a of *the Act of 29 July 2005 on public offering and conditions governing the introduction of financial instruments to the organised trading, and on public companies;*
- Article 150 and Article 151 of *the Act of 19 August 2011 on payment services.*

367. Pursuant to Article 6b(6) of *the Act of 21 July 2006 on financial market oversight*, the KNF (PFSA) also informs of criminal proceedings conducted ex officio or as a result of a notification submitted by an entity other than the KNF (PFSA), in the case of which the Chair of the KNF (PFSA) exercised the right of the injured party in criminal proceedings[109]

368. Gambling activities are regulated in Poland by *the Act of 19 November 2009 - gambling law* (Journal of Laws of 2019, item 847). In accordance with Article 3 of the aforementioned Act, arranging games of chance, betting, card games and games on gaming machines as well as conducting the activity in this scope is permitted under the relevant concession, licence or submitted registration. For criminals, illegal gambling is often a source of high income and is subsequently subject to laundering.

369. Pursuant to Article 107 § 1 of the Code of Criminal Procedure, liability under this provision is imposed on anyone who, contrary to the provisions of the Act or the terms of a licence or permit, organises or conducts gambling activities. Committing of this act in order to obtain a financial benefit from the organisation of collective participation in a gambling game is subject to more severe criminal liability (Article 107 § 3 of the kks).

370. In the Fiscal Penal Code, the behaviour consisting in selling tickets or other evidence of participation in a lottery, betting or game on a gaming machine without the right to do so is also penalised (Article 110 of the kks).

371. In the case of offences against the reliability of documents, the number of cases of committing such offences in 2017 is relatively high, accounting for approx. 7.9% of all detected offences. These offences are penalised in Articles 270 - 277 of the kk.

372. Pursuant to Article 270 of *the Penal Code* , "whoever, in order to use for an authentic document, forges or alters a document or such a document as an authentic one, shall be subject

---

[109]Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2018, Warsaw 2019, p. 233, available at: https://www.knf.gov.pl/publikacje_i_opracowania/sprawozdania.

to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for a period from 3 months to 5 years”. However, until now the execution of so-called collector's documents has not been subject to a penalty. For at least a few years, it is possible to find websites offering such documents, such as ID cards, driving licences, student cards and passports. They can be used to order the production of e.g. an ID card containing fictitious personal data or personal data of another person. Although such a collector's proof differs from the original (e.g. colour saturation, coating, low quality of the hologram, lack of impression of three-dimensional security features), these differences are difficult to find when using a scan of such a document[110] They are relatively often used to commit various types of fraud. The police warn, among other things, against using them to impersonate a user of a telecommunications operator and to defraud a duplicate SIM card (so-called *SIM-swap-fraud*). “In this way, the telephone number is taken over, which is used to pair mobile banking applications installed on the phones and to make bank transfers or take over users' e-mail or social network accounts. This gives criminals access to the authorisation or authentication of banking operations, e.g. in the form of codes received via SMS.”[111] There is also a risk that such documents may be used as authentic documents when using the products and services of obligated institutions.

373. On 12 July 2019, the majority of provisions of *the Act of 22 November 2018 on public documents* (Journal of Laws of 2019, item 53) will enter into force, including Article 58 pursuant to which: “Whoever produces, offers, sells or stores a replica of a public document in order to sell it shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty of up to 2 years.”

5.2. ESTIMATES OF PROFITS FROM CRIME SUBJECT TO LAUNDERING

374. Calculating illegal profits subject to laundering is not easy. There is a lack of sufficient data, in particular on the profits derived from committing of individual predicate offences for the purpose of money laundering in Poland as well as the data related to profits transferred to Poland from illegal activities undertaken abroad.

375. The “ECOLEF” project, funded by the European Commission (*DG Home Affairs*) and carried out by the University of Utrecht, estimated, in the same way as the above, the profits from criminal activities in individual EU Member States that could have been laundered in 2009. For Poland, this estimate amounted to about EUR 3,693 million (i.e. about 1.24% of GDP)[112]. At the same time, it was noted that the estimates were based on generally available data. Where no country-specific data were available, estimates based on data from similar countries or averages calculated for the regions[113] concerned were used.

376. Pursuant to the provisions of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism*, the GIFI received in previous years information on individual transactions provided pursuant to Article 8(3) and (3a) of this Act (the so-called STR

[110] https://chronpesel.pl/Aktualnosci/Rosnie-liczba-oszustw-na-kolekcjonerskie-dowody-osobiste, date of reading, 29 May 2019

[111] http://www.policja.pl/pol/aktualnosci/170023,Oszukuja-na-amerykanskiego-zolnierza-Inni-maja-kolekcjonerski-dowod-i-staraja-si.html, date of reading, 29 May 2019

[112] “ECOLEF” Project. The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy. Final report, Utrecht University, February 2013, p. 39.

[113] Ibidem, p. 36.

- suspicious transaction reports). One of the elements of the information was the amount of the transaction that could possibly be taken into account when considering the estimated value of illicit profits subject to laundering. In total, in 2017 the GIFI received information about the STR with a total value of approximately PLN 9.0 billion (in 2016, respectively, this value amounted to approximately PLN 10.1 billion)[114]. It should be borne in mind, however, that these values relate to transactions selected by obligated institutions which, to the best of their knowledge, may be related to money laundering or financing of terrorism. This does not mean that all reported transactions were linked to the profits generated from the committed crime.

377. On the other hand, in annual reports on the implementation of *the Act on counteracting money laundering and financing of terrorism*, the GIFI also indicated the total amount of assets described in notifications to the prosecutor's office on the suspicion of committing a money laundering offence. In 2018, it amounted to over PLN 6.3 billion, and in 2017 - to over PLN 6.3 billion. - approx. PLN 6.2 billion, while in 2016. - approx. PLN 18.6 billion[115] It should be emphasised that there is a significant difference between the data for 2017-2018 and the information for 2016. It should be noted, however, that over the past few years, i.e. in the period of 2013-2015, the total amounts of these assets remained at the level of several billion PLN annually[116]. The total amount of property values indicated in GIFI reports on suspected money laundering was particularly significantly affected by those related to suspected money laundering from fiscal offences, in particular the so-called VAT carousels. In 2016, they accounted for approximately 93.7% of the total amount, while in 2017, only about 70.2% of the total amount and in 2018 - approximately 51.8%[117].

378. In any case, it should be emphasised that GIFI notifications are not the only sources of criminal proceedings conducted by the prosecutor's offices related to suspected money laundering. Therefore, the above amounts definitely do not comprise all identified assets subject to laundering (not to mention those values derived from offences which were not detected by GIFI or law enforcement authorities).

379. For example, in 2016-2017, the Police secured (but not only in money laundering cases) for penalties, penal measures, compensation measures and forfeiture of property with the value of[118]:

- **PLN 730,717,322** in 2016 and **PLN1,453,745,554** in 2017 (the value of the property secured with suspects in proceedings **conducted[119]*** by the Police);

[114] The GIFI also received descriptive information on suspicious activity, the so-called SARs, both from obligated institutions and from cooperating units. However, they were not always accompanied by specific amounts of suspicious assets. Moreover, in the case of obligated institutions, SARs sent by them were very often connected with STRs sent simultaneously (often with many STRs).
[115] It should also be borne in mind that the suspicious transactions identified in these reports were sometimes carried out before the year in which they were sent.
[116] Respectively: in 2015 – PLN 17.1 billion, in 2014 – PLN 18.8 billion and in 2013 – PLN 16.8 billion.
[117] It may be assumed that the decline resulted indirectly from the effectiveness of the use of instruments for counteracting and detecting fiscal offences introduced in 2016-2017.
[118] The most frequently used assets being the subject of collaterals based on property were financial means accumulated in cash and real estate. According to the basis of the security, the most common types of security were: security on account of damage repair (compensatory measure), security of a fine and security of a forfeiture decision.
[119] It refers to procedural events in the form of proprietary security and recovery of property that took place in a given year, regardless of the stage of criminal proceedings.

- **PLN 1,453,745,554** in 2016 and **PLN 393,808,551** in 2017 (the value of property secured in proceedings **terminated****[120] by the Police according to the KGP Bulletin).

380. In addition, in the aforementioned period the Police recovered property with the total value of:

- PLN 483,145,584 in 2016 and PLN 468,090,112 in 2017 (the value of the property recovered in proceedings conducted by the Police);
- PLN 295,542,176 in 2016 and PLN 233,821,092 in 2017 (the value of property recovered in proceedings terminated by the Police according to the KGP Bulletin).

381. While estimating illegal profits subject to laundering, it is possible to consider referring to the detection rate, the total value of assets secured in the course of criminal proceedings and the potential ratio relating to the estimate of the share of secured assets originating from criminal activity in the total amount of all assets obtained illegally.

382. According to the data obtained from the National Prosecutor's Office, in 2017 the total value of property covered by proprietary security in cases related to money laundering initiated in 2017 amounted to PLN 530,310,152.03. At the same time, police information shows that the ratio of detected economic and criminal offences to confirmed economic and criminal offences in 2017 amounted to 68.5%.[121] However, there are no Polish data concerning the ratio relating to the estimation of the share of secured property values derived from criminal activity to the sum of all property values obtained illegally. It is worth mentioning, however, that the disadvantage of this method is first of all the reference to the amounts of proprietary collaterals in individual years, the value of which may be a result of various factors (e.g. the effectiveness of the prosecutor's office and other law enforcement agencies, amendments to legal regulations, operating procedures, etc.).

383. Since 2014, the Central Statistical Office (GUS) has been publishing revised annual data on GDP and GNI, in connection with the implementation of the new methodology (i.e. ESA2010), as well as other statistical adjustments, including those related to illegal activities. However, it stresses that it does not carry out its own surveys in the scope of calculation of profits originating from committed prohibited acts. In its estimates, the GUS relies on data from other sources, including the results of research conducted by specialist institutions and research centres as well as police reports. It indicates, however, that "the available reports and studies often focus on the social and sociological dimension of such activities rather than on the measurement of economic variables, therefore, they do not respond directly to the needs of national accounts and thus require a multi-dimensional analysis and a very careful interpretation"[122].

---

[120] Applies to the value of total proprietary security in cases which were concluded in a given year. Data on terminated cases are published in the Statistical Bulletin of the Bureau of Intelligence and Criminal Information of the Police Headquarters.

[121] The ratio was calculated on the basis of data on criminal offences and economic crime (summing up the detected offences from both categories and calculating their share in the total number of confirmed offences) http://statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-kryminalne/63470,Przestepstwa-kryminalne-ogolem.html, http://statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-gospodarcz/122291,Przestepstwa-gospodarcze.html, access 25 June 2018.

[122] Memo - Implementation of the European System of National and Regional Accounts in the European Union (ESA2010) into the Polish National Accounts. Methodological changes and their impact on the main

384. In accordance with Eurostat requirements, the GUS estimates GDP by adding revenues from the so-called unobserved economy, comprising the shadow economy and illegal activities. The shadow economy is defined by Eurostat as comprising "all legal production and provision of goods and services that are deliberately concealed from public authorities for the following four reasons:

1) To avoid payment of income, value added or

other taxes, 2) To avoid payment of social security

contributions, 3) To avoid having to meet certain legal standards such as minimum wages, maximum hours,

safety standards, etc., and 4) To avoid complying with certain administrative procedures, such as completing statistical questionnaires or other administrative forms"[123]. Illegal activities, on the other hand, involve primarily profits in the areas of sexual services, drug production and trafficking, alcohol and tobacco smuggling. The GUS points out that in this way illegal activity should be understood exclusively as activity related to criminal activity, whereas, for example tax evasion is an activity within the shadow economy.

Table 16 - Impact of activity associated with prostitution, drugs and cigarette smuggling activities in the years 1995-2013, current prices in PLN million (source: GUS)[124]

Item	1995	2000	2010	2011	2012	2013
GDP without illegal activity	337,222	744,378	1,416,585	1,528,127	1,596,378	1,635,745
Illegal activities	**2,202**	**3,605**	**9,434**	**10,679**	**12,662**	**13,021**
Prostitution (security/pimps activity)	78	187	659	649	657	657
Drugs	1,826	2,837	7,247	7,938	9,752	9,840
Cigarette smuggling	298	581	1,528	2,092	2,253	2,524
GDP with illegal activities	339,424	747,983	1,426,019	1,538,806	1,609,040	1,648,766
Share of illegal activities in GDP	**0.65%**	**0.48%**	**0.66%**	**0.69%**	**0.79%**	**0.79%**
Prostitution (security/pimps activity)	0.02%	0.03%	0.05%	0.04%	0.04%	0.04%
Drugs	0.54%	0.38%	0.51%	0.52%	0.61%	0.60%
Cigarette smuggling	0.09%	0.08%	0.11%	0.14%	0.14%	0.15%

385. Adjusted GDP data by attaching estimates of the size of unobserved economy are presented by the GUS in the reports on national accounts by sectors and institutional sub-sectors in particular years.

macroeconomic aggregates, GUS Department of National Accounts, Warsaw, 29 September 2014, p. 12 (Annex No. 1: Illegal activity in Poland - methodological assumptions and results of estimations).
[123]Ibidem, p. 13.
[124]Ibidem, p. 17.

Table No 17 - Estimates of the size of the shadow economy and illegal activity in GDP generation in 2013-2016 (current prices)[125].

Item	2013	2014	2015	2016
in PLN million				
GROSS DOMESTIC PRODUCT (including unobserved production)	1,656,895	1,719,769	1,799,392	1,858,468
in percentage				
GROSS DOMESTIC PRODUCT (including unobserved production)	100	100	100	100
Total unobserved economy	**13.8**	**13.3**	**13.5**	**13.2**
including:				
- shadow economy	13.0	12.7	13.2	12.9
• in registered entities	*10.6*	*10.4*	*11.0*	*10.8*
• due to performing non-registered work	*2.4*	*2.3*	*2.2*	*2.1*
• illegal activities	0.8	0.6	0.3	0.3
• pimping	*0.04*	*0.05*	*0.04*	*0.04*
• drugs	*0.60*	*0.46*	*0.24*	*0.25*
• cigarette smuggling	*0.15*	*0.11*	*0.06*	*0.04*

386. In the case of pimping income, it was estimated by multiplying the number of sex workers (including non-residents), the number of contacts during the year and the average price of services. Estimates of drug production and trafficking include those drug groups which are most relevant to the Polish market (i.e. marijuana and hashish, amphetamine, cocaine and crack, heroin, ecstasy, LSD and hallucinogens and Polish heroin). On the other hand, in the scope of estimation of income from cigarette smuggling, the following activities were mainly taken into account:

- smuggling of cigarettes from the East and their illegal sale in trade (mainly in bazaars);
- export of cigarettes legally manufactured in Poland to Western European countries for the purpose of their sale without excise duty marks mandatory there;
- illegal industrial-scale cigarette production associated with counterfeiting of well-known brands.

Part of the revenue associated with legally manufactured cigarettes has been classified as shadow economy[126]

387. When analysing these figures, it is important to note a significant decline in the share of revenues from illicit drug production and trafficking in GDP in 2014 and 2015 as compared to previous years. Moreover, the share of cigarette smuggling revenue in GDP decreased in the

---

[125] National Accounts by institutional sectors and subsectors in 2013-2016, GUS, Warsaw 2018, p. 282 (Annex 3: Shadow economy and illegal activity in national accounts), available at: https://stat.gov.pl/obszary-tematyczne/rachunki-narodowe/roczne-rachunki-narodowe/rachunki-narodowe-wedlug-sektorow-i-podsektorow-instytucjonalnych-w-latach-2013-2016,4,13.html.
[126] Ibidem, p. 281.

years 2014 - 2016. The above-mentioned declines had an impact on the share of estimated revenues from illegal activities in GDP over this period. Due to the fact that GUS does not take into account profits from other types of crimes when estimating them, it cannot be clearly indicated on this basis that the level of profits from illegal activity, which could have been subject to laundering, has indeed decreased.

388. The GUS estimated the share of illegal activity in the GDP for each indicated year below 1%, while the share of the shadow economy in the GDP was relatively high (between 12.7% and 13.2% annually in 2013-2016). It should be stressed, however, that the revenue from illegal activities has been limited to only three categories of offences. Moreover, a considerable part of fiscal offences (related to tax fraud, including VAT carousels), which are often committed in connection with the functioning of organised crime, has been classified as shadow economy.

389. Alternative estimates of income from the unobserved economy were provided by the Institute for Studies on Market Economy (IBnGR). According to its estimates, the share of revenues from the unobserved economy in GDP in individual years in the period 2012-2016 ranged from 19.2% to 21.2%. In the table below, the IBnGR adjusted the GUS estimates for 2012-2013 and for 2014-2015 it presented its own estimates, including the forecast for 2016. According to its estimates, in 2012-2015 the average share of the shadow economy in GDP reached approximately 19.9%.

Table No 18 - Estimates of the size of the shadow economy (according to IBnGR approach) in Polish economy in 2012-2016 (PLN billion)[127].

	2012	**2013**	**2014**	**2015**	**2016**
Unobserved economy (GUS) *)	228	240	234	240	260
including:					
Shadow economy (1)	215	227	220	226	245
Illegal activities (2)	13	13	14	14	15
IBnGR reassessment (3)	**147**	**112**	**126**	**129**	**139**
Shadow economy (IBnGR approach) (1+2+3)	375	352	360	368	399
GDP adjusted for the shadow economy according to the IBnGR approach	1776	1768	1845	1919	2027
Share of the shadow economy in the adjusted GDP	21.1%	19.9%	19.5%	19.2%	19.7%

**) GUS data until 2013, from 2014 - IBnGR estimates.*

390. The IBnGR uses the term “shadow economy zone” (in short, “shadow economy”) as a synonym for the unobserved economy, which is composed of 3 basic elements, i.e:

- “illegal activities where both parties are voluntary partners in business transactions”;
- “hidden activities, where transactions as such are not illegal but are not reported in order to avoid administrative procedures”;
- “activities defined as “informal”, usually when no records are kept”[128]

[127] Jacek Fundowicz, Krzysztof Łapiński, Marcin Peterlik, Bohdan Wyżnikiewicz, Theshadow economy in the Polish economy in 2016, IBnGR, Warsaw, March 2016, p. 20, available at: www.ibngr.pl/content/download/2173/20176/file/Szara strefa 2016.pdf.
[128]Ibidem, p. 6.

At the same time, it defined the area referred to as the shadow zone by the GUS as the "shadow economy".

391. According to the information provided by the IBnGR, its estimates cover a wider range of activities classified as the shadow economy than in the case of the GUS (which ignored, among others, the estimates of understatement of turnover by larger enterprises, illegal gambling, illegal trading in fuel, part of bazaar trade and cross-border trade as well as e-commerce). In order to estimate the revenues from illegal activities for the years 2014-2016, the IBnGR assumed the share of 0.8% of GDP (adequately to the estimates of the GUS for 2012-2013)[129]

392. Other estimates of the shadow economy (understood as in the case of the IBnGR) were presented by the Institute of Economic Forecasting and Analysis (IPAG).

Table No 19 - Estimates of the size of the shadow economy (according to IPAG approach) in the Polish economy in 2015-2019 (PLN billion)[130]

	2015	**2016**	**2017**	**2018**	**2019**
Unobserved economy (GUS) (1)[*)]	243	246	263	273	294
IPAG reassessment (2)	127	133	135	132	130
Shadow economy (IPAG approach) (1+2)	370	379	397	405	424
PKB skorygowany o szarą strefę w ujęciu IPAG	1,927	1,994	2,124	2,248	2,464
Share of the shadow economy in the adjusted GDP	19.2%	19.0%	18.7%	18.0%	17.2%

**) GUS data until 2016, from 2017 - IPAG estimates.*

393. According to IPAG, in the examined period, the total value of the shadow economy (in absolute amounts) will year by year, reaching the equivalent of ca. PLN 424 billion in 2019. On the other hand, its share in the GDP will fall to 17.2% of GDP in 2019. The IPAG indicated the following reasons for this decline:

- "the favourable economic climate encouraging companies to carry out activities unconcealed from the public authorities (the GDP growth rate forecast by IPAG in 2019 is 3.8 per cent)";
- "the authorities' activities aimed at tightening of the tax system and, in particular, at collecting VAT (mainly in the fuel sector)";
- "effective combating of illegal activities - reduction of production and trafficking of drugs and designer drugs, reduction of cigarette smuggling, elimination of illegal gambling".[131]

394. Estimates of the shadow economy can be calculated using different methods (which, however, may give divergent results). Five basic methods were presented by Professor Friedrich Schneider in one of his works, i.e.:

- the discrepancy method (estimation using the system of national accounts statistics);

---

[129] Ibidem pp. 19-20.
[130] Jacek Fundowicz, Krzysztof Łapiński, Marcin Peterlik, Bohdan Wyżnikiewicz, Shadow economy, 2019, IPAG, Warsaw, March 2019, p. 24, available at: www.ipag.org.pl/Content/Uploaded/files/IPAG_Szara_Strefa_2019.pdf.
[131]Ibidem, p. 25.

- micro method (techniques on a representative social group in order to obtain, among others, information on the general perception of the shadow economy by the society);
- micro method - use of questionnaires addressed to the management staff;
- micro method - estimates based on the gap between household income and the value of household consumption;
- the MIMIC method (of both the macro type and the so-called adjusted MIMIC method)[132]

395. Using the last method, Professor F. Schneider indicated that the estimated size of the shadow economy in Poland in 2017 amounted to approx. 22.2% of GDP (excluding the adjustment typical of the revised MIMIC method, i.e. deductions for legally purchased materials for the shadow economy purposes, neighbourhood aid, do-it-yourself and illegal activities)[133]

396. Comparing the estimates presented above by both GUS, IBnGR, IPAG and by Professor F. Schneider, it is clear that they differ significantly from each other (e.g. for 2015, according to the GUS, it was about 13.5% of GDP and according to the IBnGR - 19.2% of GDP, while for 2017, according to the IPAG, it was 18.7% of GDP, and according to Professor F. Schneider - 22.2% of GDP). In addition, it should be noted that the estimation of the shadow economy takes into account activities which, at the first glance, do not have much to do with criminal activity.

397. While presenting its estimates, the IPAG listed those areas that it took into account when reassessing the value of the unobserved economy.

Table No 20 - Major activities excluded or not fully included in the official estimates[134]

	Section	Type of activity
A	Agriculture, forestry, hunting and fishing	• seasonal agricultural work
		• illegal logging and sale of trees
		• sale of forest fleece
		• poaching
B	Mining and quarrying	• illegal coal mines
		• sand and gravel extraction
C	Industrial processing	• production of alcohol and tobacco products
		• manufacture of clothing
		• production of counterfeit medicines
E	Water supply, sewage and waste management, reclamation	• illegal waste management
		• trading in used motor oil
F	Construction	• unregistered construction works
G	Trade; repair of vehicles	• illicit trafficking in arms

132 The description of these methods can be found in: Friedrich Schneider, Implausible Large Differences in the Sizes of Underground Economies in Highly Developed European Countries? A Comparison of Different Estimation Methods, Working Paper No. 1709, Department of Economics, Johannes Kepler University of Linz, June 2017.

133 Ibidem p. 14 (Figure 2.3: Size of the shadow economy of 31 European countries in 2017 - macro and adjusted MIMIC estimates).

134 Jacek Fundowicz, Krzysztof Łapiński, Marcin Peterlik, Bohdan Wyżnikiewicz, Shadow economy, 2019, IPAG, Warsaw, March 2019, p. 26, available at: www.ipag.org.pl/Content/Uploaded/files/IPAG_Szara_Strefa_2019.pdf.

		• untaxed street trading
		• untaxed electronic commerce
		• trade in fuels from various sources, including smuggling
		• vehicle repair and maintenance
		• frontier trade
		• commission services
		• fraudulent sales on the Internet
		• trafficking in counterfeit medicines
		• illegal import of medicines from Poland
		• unregistered sales at mass events, including concerts of popular music
H	Transportation and Storage	• unlicensed passenger transport (so-called passenger transport)
		• overcharging
I	Accommodation and catering	• unregistered accommodation and catering services
		• tips
		• delivery of food to apartments and offices
J	Information and communication	• unregistered IT services
		• illegal copying and distribution of copyrighted content (computer piracy, making illegal copies of films and music available against payment, photocopying of books)
K	Financial and Insurance Activities	• usury
		• currency trading
L	Real estate service	• rental of immovable property and premises
		• land lease
M	Professional, Scientific and Technical Activities	• legal services (legal advice)
N	Administration and support	• financial services (e.g. filling in PIT for a fee)
		• advisory services, intermediation (e.g. car sales, out of commission)
P	Education	• tutoring
		• writing diploma theses
Q	Human Health and Social Work Activities	• healers, chiropractors
R	Arts, entertainment and recreation activities	• unregistered/illegal gambling, online betting
		• ticketing (secondary market)
		• underestimated income of music bands
S	Other services	• illegal parking and unauthorised collection of parking fees
T	Households as employers of domestic personnel, undifferentiated goods and services-producing activities of households for own use	• care of children, elderly and disabled people
		• home help
		• paid neighbourhood assistance

398. It should be noted that a considerable part of the above-mentioned activities - as well as the part of them that was taken into account by the GUS - is related to gaining income without disclosing it to the tax authorities. This is often the most legal activity. Only the failure to report

such activity to the tax authorities and the failure to pay the relevant taxes and contributions required by law is illegal.

399. This means, however, that such income - classified as benefits derived from the shadow economy - cannot be considered as proprietary benefits derived from a prohibited act, which may be subject to laundering. At most, this category may include that part of them which, in accordance with the law, should be transferred to the State Treasury or for other purposes. In reality, therefore, only part of the estimates related to the shadow economy can be included in the estimates of illegal benefits that may be subject to money laundering. In addition, it is worth emphasising that at least some of the above mentioned estimates do not take into account the whole spectrum of illegal activities and benefits that may be obtained from them (e.g. in the GUS, in its estimates - according to the Eurostat methodology - refers to 3 basic types of crimes). It therefore appears that estimates relating to the shadow economy should be treated with great caution as regards the estimation of the benefits derived from illegal activities that may be subject to money laundering.

400. Based on GUS data (and IBnGR estimates) presented in Table 18 above, entitled *Estimates of the size of the shadow economy (in terms of IBnGR) in the Polish economy in 2012-2016*, the average share of profits from illegal activity in the total estimated value of the unobserved economy in 2012-2016 can be calculated. It reached approximately 5.74%. Taking this percentage as a fixed percentage determining the ratio of profits from illegal activities to the total estimates of the shadow economy and comparing it with the estimation of the shadow economy in Poland by Professor F. Schneider for 2017 (calculated according to the MIMIC method), which are the largest among the presented above, one can estimate profits from illegal activity at approx. 1.27% of GDP, i.e. approx. 25.3 billion PLN. For comparison, on the basis of professor's data for 2016[135] - profits from illegal activities could be estimated at about 1.32% of GDP, i.e. about PLN 24.5 billion.

401. If the above mentioned ratio is applied to IPAG data on the grey market in the adjusted GDP, one could estimate the profits from illegal activity at approx. 1.09% for 2016, approx. 1.08% for 2017, 1.04% for 2018 and approx. 0.99% for 2019.[136] Therefore, it can be assumed with a high probability that the estimates based on the IPAG data may constitute the bottom limit and the estimates based on the data of Professor F. Schneider - the top limit of the range in which the total income earned by criminals is included (for 2016 it would range from about 1.09% to about 1.32% of GDP, and in 2017 - to about 1.32% of GDP and in 2017 from approx. 1.08% to approx. 1.27% of GDP).

5.3. RISK AREAS ON THE MARKET

402. The threats in the area of money laundering and financing of terrorism can generally be divided into risks occurring in the financial market and outside this market. However, it should

---

[135] Friedrich Schneider, Estimating the Size of the Shadow Economies of Highly developed Countries: Selected New Results, in: CESifo DICE Report 4/2016, December 2016, p. 48.

[136] Eurostat is working on the development of a methodology for estimating the value of assets subject to laundering. In 2018, he published, among other things, the study entitled *Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments*, which is intended to harmonise the rules for collecting data and compiling statistics on illegal economic activity.

be borne in mind that they are often linked with each other, in particular in cases where providers of services or products outside the financial market which may be used to commit the above-mentioned offences are directly or indirectly linked to the execution of financial transactions carried out through financial market institutions.

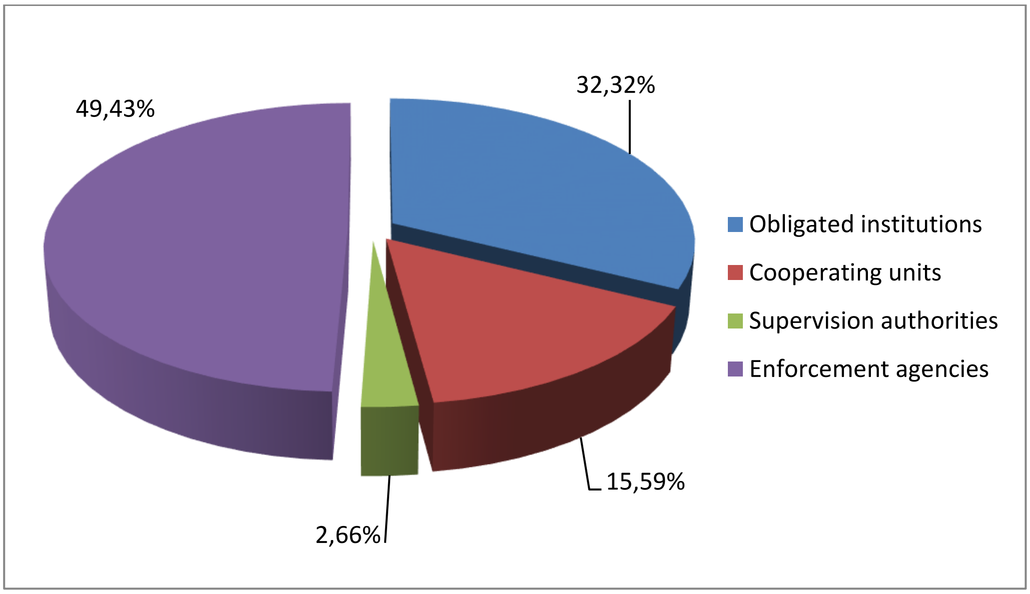
403. It is also worth remembering that some risks are common to all entities, both those operating within and outside the financial market. In particular, it is important to bear in mind the risk that criminals may use the employees of these entities to help in money laundering and financing of terrorism or their activities to mix income from legal and illegal sources.

5.3.1. Risk areas on the financial market

404. In the second half of 2017, the GIFI asked obligated institutions[137] and cooperating[138] units to fill in questionnaires in order to gather information on their perception of money laundering and financing of terrorism issues and counteracting of these offences. The questionnaires were divided into 4 types, separately for obligated institutions, law enforcement agencies, supervisory authorities and other cooperating units.

405. The total of 263 responses were received. Most of them originated from cooperating entities.

Figure no. 5 - Breakdown of responses to questionnaires according to categories of entities



406. The questionnaires were filled in by representatives of individual entities on the basis of their knowledge and experience as well as information available in the particular entity. The answers indicated by them show that about 74.1% of persons had experience with counteracting or combating criminal activity (including money laundering and financing of terrorism) for at

[137] The questionnaire was made available to all obligated institutions to complete it by publishing it on the secure website of the GIFI.

[138] The questionnaires were sent to selected ministries, courts of appeal, UKNF (PFSA office), NBP, National Credit and Savings Union, ABW, CBA, Police (including CBŚP), Border Guard, military services, revenue administration regional offices, customs and tax control offices, governors of provinces and several other authorities.

least 2 years, about 4.9% - shorter than 2 years, about 17.9% indicated the lack of experience in this area and about 3.0% of persons did not provide an answer in this respect.

407. Only 85 replies were received from obligated institutions. Most of them were submitted by banks (about 70.1%), notaries (about 11.8%), as well as cooperative savings and credit unions (about 7.1%). Other obligated institutions included postal operators, entrepreneurs conducting factoring activity, currency exchange, investment companies, payment institutions and other financial institutions.

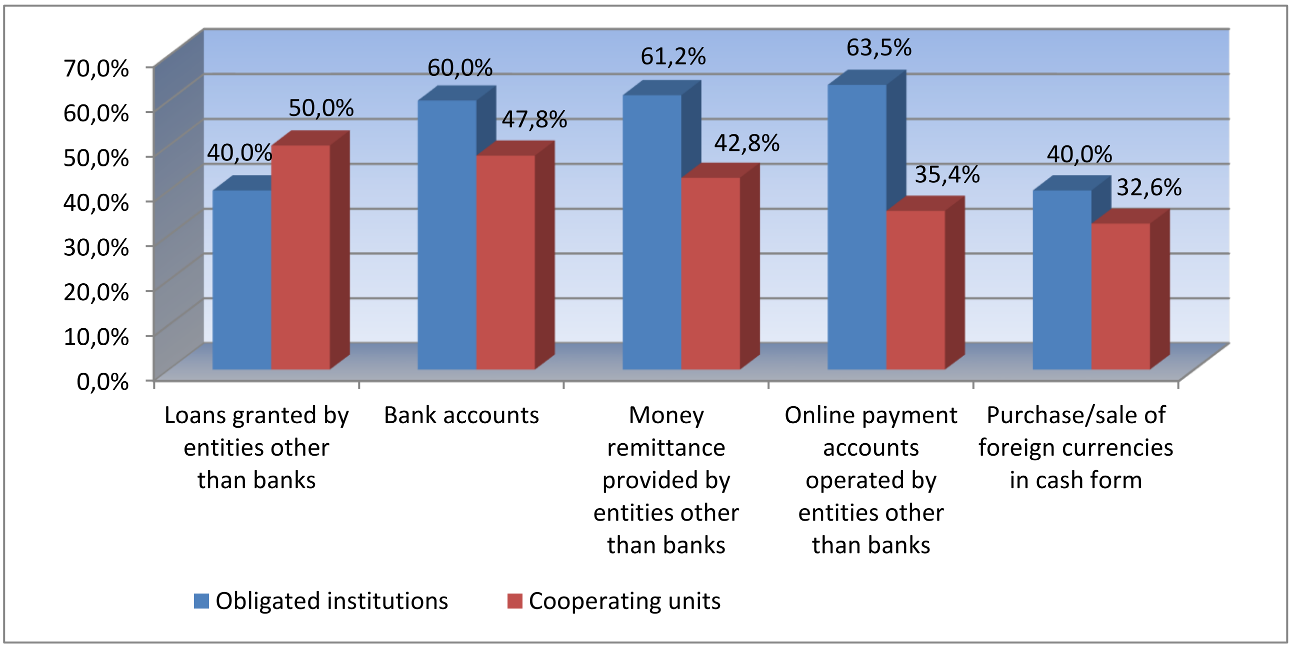
408. All types of questionnaires included a request to identify 5 products and services offered on the financial market which are or could be most frequently used for money laundering. Answers were selected from the list containing the following items:

- bank accounts;
- credits and loans granted by banks;
- payment services provided by banks;
- money remittance services provided by entities other than banks;
- online payment accounts maintained by entities other than banks;
- other payment services provided by entities other than banks;
- services within the so-called underground banking system (*Hawala* type);
- credit and debit cards;
- prepaid cards;
- virtual payment cards (e.g. for so-called MOTO transactions - Mail Order & Telephone Order);
- letters of credit;
- guarantees;
- payment collection;
- traveller’s cheques;
- other checks;
- bills of exchange;
- participation units in investment funds;
- securities;
- derivatives;
- lease;
- factoring;
- loans granted by entities other than banks;
- purchase/sale of foreign currencies in cash;
- purchase/sale of foreign currencies in a non-cash form;

- purchase/sale of foreign currencies using an automatic device;
- services provided on the FOREX market;
- securities accounts and cash accounts used to service them;
- unit-linked life insurance;
- other financial products and services.

409. The list of 5 products and services indicated by the largest number of institutions is identical with the list of 5 products and services indicated by the largest number of cooperating entities. They differ only in terms of their order. In the case of the obligated institutions, the largest number of replies referred to online payment accounts operated by entities other than banks, followed by money remittance services provided by entities other than banks, bank accounts, loans granted by entities other than banks and the purchase/sale of foreign currency in cash. On the other hand, the replies of the cooperating entities showed that the most commonly used money laundering activities were loans granted by entities other than banks, followed, respectively, by bank accounts, money remittance services provided by entities other than banks, online payment accounts held by entities other than banks and purchase/sale of foreign currencies in cash.

Figure No. 6 - Responses concerning products and services offered on the financial market most frequently used for money laundering



410. It is worth emphasising that the choice of virtual currencies was possible in the question concerning the indication of 5 products and services offered outside the financial market which are or may be most frequently used for money laundering. In response to this question, the largest number of obligated institutions and the largest number of cooperating units indicated the use of virtual currencies (respectively, 45.5% of answers from cooperating units and 62.4% of answers from obligated institutions).

411. Summing up, both cooperating units and obligated institutions which submitted their answers to the survey questions indicated that the most frequently used money laundering products and services are virtual currencies, banking, payment services, currency exchange and lending activity. The risks associated with these areas as well as with the financial market areas specified in the 2017 Report of the European Commission on the transnational assessment of the risks of money laundering and financing of terrorism in the EU, are described below[139]

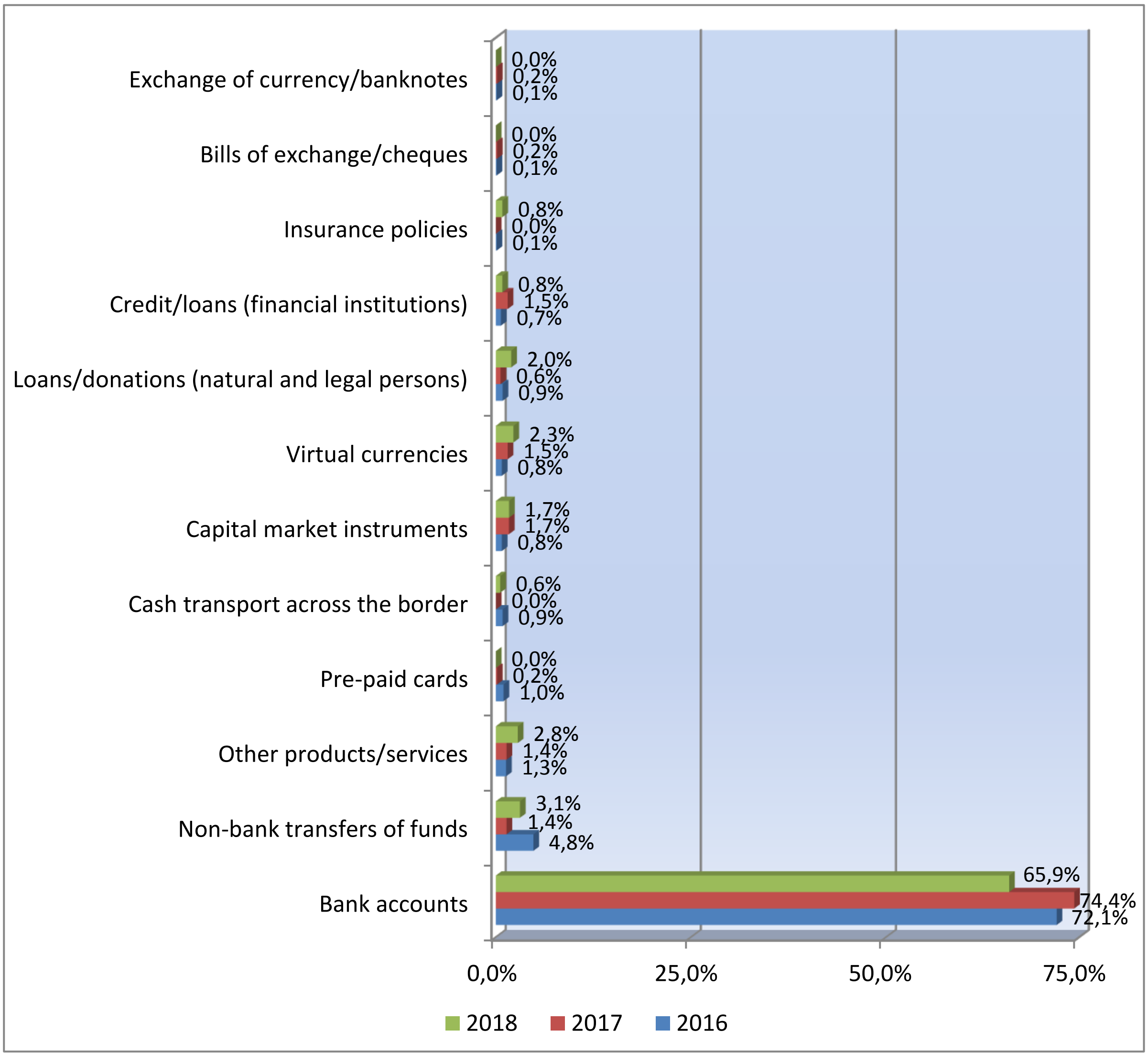
Banking

412. Pursuant to Article 5(1) of *the Act of 29 August 1997 - Banking Law* provides for specific types of activities[140] to be performed only by banks although this does not mean that the scope of the products and services they offer is limited. In any event, a considerable part of their offer is related to the maintenance of bank accounts.

[139] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 June 2017, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[140] i.e.: accepting cash deposits payable on demand or at a specified date and maintaining such deposits accounts; maintaining other bank accounts; granting loans; granting and confirming bank guarantees and opening and confirming letters of credit; issuing bank securities; conducting bank monetary settlements; as well as performing other activities provided for exclusively for the bank in separate acts.

Figure No. 7 - Completed analytical proceedings instituted by the GIFI in 2016-2018, broken down by products and services used for execution of suspicious transactions (according to data as of 31 December 2018)



413. The analysis of information on the typology of completed analytical proceedings[141] initiated by the GIFI in 2016-2018 shows that the majority of them concerned suspicions of money laundering or financing of terrorism related to the use of bank accounts for suspicious transactions (in 2016 - about 72.1% of such proceedings, in 2017 - about 74.4%, and in 2018 - 65.9%)[142].

414. Opening a bank account and executing transactions through it (including so-called cross-border transactions) is relatively simple. The risk of using bank accounts is not only related to cash transactions which enable introducing money originating from crime into the financial

[141] i.e. concluded with the submission of a notification to the public prosecutor's office or information to another authorised public administration body / unit in accordance with the provisions on counteracting money laundering and terrorist financing. Analytical proceedings were initiated on the basis of information from both obligated institutions and cooperating units.

[142] According to the information on analytical proceedings, recorded in the GIFI IT system on 31 December 2018.

market. It should be remembered that in the contemporary world, committing a predicate offence for money laundering often involves obtaining money already present in non-cash circulation (e.g. coming from various types of fraud and extortion).

415. The risk of money laundering and financing of terrorism linked to bank accounts is mainly affected by the following elements:

- possibility of executing so-called cross-border transactions (i.e. execution of transactions outside the country where the account is maintained);
- relatively fast transfer of funds;
- possibility of executing cash transactions (both for the purpose of crediting the account and debiting it);
- relatively fast and easy access to a bank account and execution of transactions through it via a telecommunications network (using the Internet, telephone lines);
- possibility of appointing proxies to accounts, executing transactions on behalf of its owner.

416. An important element of the offer is the access to the account via electronic communication channels (in particular via the Internet), which facilitate the concealment of data of the actual payers of the transaction (especially if "straw men" and "shell companies" are used for this purpose[143]). According to the NBP statistics[144], the total number of non-cash transactions is steadily increasing year on year. In the first half of 2018 there were over 3.5 billion of such transactions (i.e. approx. 15.1% more than in the first half of 2017 and approx. 6.6% more than in the second half of 2017) while transfers[145] constituted over 37.4% of this number.

417. Within the framework of maintaining bank accounts, various additional services are often offered. One of them is a service often called the *collect* service or identification of mass payments. In general, the aforementioned service consists in providing the bank's customer with the possibility to generate numbers of so-called virtual accounts (created in accordance with the NRB standard[146]), behind which in reality one settlement account of the bank's customer is hidden. Within its scope, the bank's customer obtains a possibility to distribute these numbers among his counterparties in order to execute transactions for the bank's customer. A counterparty executes transactions for a bank customer using a dedicated virtual account number or virtual account numbers. Transactions are, in fact, booked on the actual settlement account of the bank's customer.

418. The *collect* service - used more and more frequently not only by entrepreneurs with multiple individual recipients of their products or services but also by other entities - hinders the analysis of financial flows and access to knowledge about the actual payer and recipient of the transfer, in particular in the case of using information resulting from transfer orders or the

---

[143] These concepts are explained in Chapter 5.4. in the context of the money laundering methods used.
[144] Assessment of the functioning of the Polish payment system in the first half of 2018, NBP, November 2018, p. 90, available at: https://www.nbp.pl/systemplatniczy/ocena/ocena2018_1.pdf.
[145] This number refers to credit transfers carried out within the following systems: SORBNET2, TARGET2-NBP, Elixir, Euro Elixir, Express Elixir, BlueCash, BLIK and inter-branch and intra-branch transfers.
[146] i.e. the standard for the numbering of bank accounts in Poland (see provisions of Chapter IV of *Regulation No. 7/2017 of the President of the National Bank of Poland of 20 February 2017 on the method of numbering banks and bank accounts* - Official Journal of the NBP item 3).

history of accounts of bank customers' counterparties. It enables both customers' payments and withdrawals from a given account. The accounting scheme and the scope of information provided to the bank in many cases makes it impossible to monitor and analyse transactions of individual clients on an ongoing basis and, in justified cases, to examine the origin of property values at the disposal of a given client. The *collect* service provided to payment service providers generates a significant risk of money laundering, despite the fact that such entities are obligated institutions. Low barriers of entry into the payment service industry, combined with a high risk appetite and acceptance of reputation loss indicate that due to the wide range of services that can be provided, operators in the sector can be used or even deliberately set up by criminal groups in order to introduce assets from illegal or undisclosed sources into circulation.

419. Credits and loans offered by banks also pose risks in the scope of money laundering. Apart from the possibility of using "straw men" and "shell companies" to borrow and thus extort money from banks, i.e. committing a predicate offence for money laundering, there are other risks associated with them. Above all, loans and credits can be repaid from profits coming from illegal sources. Moreover, funds from credits and loans granted may be transferred - as profits from legal sources - to third parties.

420. Other products on the Polish market which may be associated with the risk of money laundering include electronic money instruments, in particular prepaid cards. The NBP conducted a detailed analysis of the prepaid cards market in Poland[147]. In the report presenting the results of this analysis, the NBP referred, among others, to their classification, objectives for which they are issued as well as related risks.

421. Prepaid cards are classified primarily with regard to their intended use[148], i.e:

- issued for the use in limited or closed networks (*closed loop* / *semi-open loop prepaid cards*);
- general-purpose prepaid cards, including *general purpose non-reloadable prepaid cards* or *general purpose reloadable prepaid cards*.

422. The former may be used only for the purchase of goods or services in the specific shop, chain or shopping centre or for the purchase of specific goods or services, irrespective of the geographical location of the point of sale. Examples of such prepaid cards are gift cards, e.g. issued by specific retail chains, membership cards, fuel cards for use in the specific service station chain, meal vouchers. Sometimes the aforementioned cards are anonymous (especially in the case of gift cards). However, due to their limited use, the risks associated with them are low.

423. General purpose prepaid cards are widely used. These cards can be used to pay salaries, pay various types of additional benefits to employees, as incentive cards or as cards used to

[147] The study entitled "Prepaid cards on the Polish market" was prepared by the Payment System Department of the NBP and presented to the Payment System Council (a consultative and advisory body acting at the NBP Management Board) as a discussion material at the Council meeting on 11 June 2018. This study has not been published by the NBP.

[148] Based on the publication of the European Commission: Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, Strasbourg, 5 July 2016, p. 148.

settle expenses during business trips as well as to pay social benefits, scholarships or pocket money and to make payments for online purchases.

424. General purpose prepaid cards may be issued by banks or non-banking payment service providers, e.g. electronic money institutions. Prepaid cards may be either a scriptural (bank) money carrier and in such a case they are debit cards or an electronic money carrier. Pre-paid cards issued in Poland by domestic banks are only debit payment cards. They constitute a payment instrument generally linked either to a standard payment account or to an account with limited functionality, i.e. used exclusively for the processing of payment orders processed through a card and for recording the means of payment credited to the account to cover future payment transactions. Data concerning this type of cards are reported to the NBP. The risk of money laundering associated with prepaid cards issued by domestic banks is low, lower than in the case of traditional debit cards (due to applicable limits on transactions, reloads or the total value of funds held on a payment instrument at any given point in time)[149].

425. According to the NBP information presenting data reported by national banks, at the end of 2018 there were 2,563,448 prepaid cards in circulation (being a kind of debit payment cards), which accounted for approx. 6.2% of all payment cards[150]. They are issued in Poland by a relatively small number of institutions (in 2017 they were issued by 10 banks). The number of transactions executed with prepaid cards in 2018 reached over 23 million. However, it was a small fraction of the total number of transactions made with payment cards - about 0.4%. In addition, the total value of prepaid card transactions was relatively low compared to the total value of all card transactions (approx. 0.5% in 2018)

426. In the opinion of the Wolfsberg Group[151] and the FATF[152], the risk of money laundering and financing of terrorism related to prepaid cards in general is primarily affected by the following elements related to them:

- possibility of executing so-called cross-border transactions (i.e. execution of transactions outside the country where the card was issued);
- the speed of transferring the funds;
- possibility to easily move cards across the border (without declaring, as in the case of cash transport).

---

[149] The lower risk compared to traditional debit cards results from the fact that prepaid cards are generally subject to stricter rules than debit cards. They are defined in a contract between the issuer-bank and the direct purchaser of the card. An actual prepaid card user may only use the funds credited to the card account (e.g. by the card buyer - a parent, an employer). Depending on the user (natural person or business entity) and the purpose for which the card is issued (e.g. pocket money or salary, social benefit or business trip), different types of restrictions may be imposed. They concern e.g. the limit of one-time funds available on the card (in the case of a card issued to the parent's/business subaccount, usually lower than the balance of the payment account supplying it), the permitted monthly reload limit, a limited source of reloads (e.g. only from the account of a given company), quantitative and quantitative limits of non-cash and cash transactions.

[150] http://www.nbp.pl/home.aspx?f=/systemplatniczy/karty_platnicze.html, data odczytu 25.04.2019 r.

[151] Wolfsberg Guidance on Prepaid and Stored Value Cards, October 2011, available at: https://www.wolfsberg-principles.com/publications/wolfsberg-standards.

[152] FATF Guidance for a Risk-based Approach to Prepaid Cards, Mobile Payments and Internet-based Payment Services, June 2013, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html.

427. In the case of anonymous prepaid cards, according to the FATF opinion, the assessment of the aforementioned risk is also influenced by such factors such as:

- potential lack of direct contact with the cardholder;
- potential lack of identification documents or the failure to verify them;
- high level of transferability owing to universal acceptability;
- possibility of recharging (in the case of multiple recharge cards);
- potential possibility of cash loading of cards;
- possibility of cash withdrawals.

428. The possibility to issue anonymous prepaid cards (without identifying and verifying the customer) applies only to electronic money storage media, although there are certain restrictions in this respect, linked to the limits of the amounts held on the payment instrument and to the limits of the amounts of transactions. Issuance of anonymous prepaid cards in Poland - electronic money carriers - is limited by the regulations resulting from Article 38 of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. It should be stressed that these rules are currently more restrictive than the regulations set out in Directive 2015/849. Currently, domestic banks do not issue prepaid cards which would represent electronic money instruments.

429. Pre-paid cards, including anonymous pre-paid cards, are issued by foreign electronic money institutions offering their products and services on a cross-border basis in Poland on the basis of a European passport. These entities are subject to home country supervision and do not report to the NBP on the number of cards issued and the volume of electronic money issued. The scale of this activity is therefore unknown. Therefore, it is difficult to assess the probability and level of occurrence of the risk of money laundering or financing of terrorism in Poland with the participation of anonymous electronic money instruments. It should be borne in mind, however, that the countries of origin of electronic money institutions also apply EU regulations on counteracting money laundering and financing of terrorism.

430. In order to ensure the development of prepaid cards and electronic money instruments on the Polish market, which would take into account the need to guarantee an appropriate level of security of transactions executed with their use, in particular in the area of money laundering and financing of terrorism, in July 2018, the Payment System Council (an advisory body acting under the NBP Management Board) established the Task Force for prepaid cards. The aim of the Team is to develop proposals for a uniform approach to the issue of electronic money on the Polish market as well as proposals for legislative, self-regulatory, educational and promotional activities necessary for the development of prepaid cards and electronic money instruments on the Polish market, ensuring an appropriate level of their security. The above proposals will be presented in the report on the activities of the Task Force at one of the meetings of the Payment System Council in 2019.

431. The risk of money laundering is also associated with loans and credits granted by banks. Although they may be used to commit a predicate offence for money laundering, in particular to extort them on the basis of forged documents, they may also be used to launder money derived from illegal activities.

432. Above all, loans and credits can be repaid using the money coming from illegal sources. Collaterals may also be established on assets obtained illegally, which are then used to satisfy claims of the bank in connection with receivables resulting from the granted loan.

433. Another service provided by banks, which is not exclusively reserved for them, is the provision of safe-deposit boxes to customers. Safe deposit boxes enable storing not only cash but also other property values of relatively small size. They can be used to hide the proceeds of crime (in various forms, not only money). An important issue related to the risk of using this service for money laundering is the inability of banks to objectively assess the type of items stored therein as well as their actual value.

Payment services

434. Although the largest number of payment transactions is still carried out through banking sector institutions, the volume of transactions carried out by domestic payment institutions (DPI) and offices of payment services (OPS) is growing year by year[153]. In 2018 Q2 it increased by approx. 42.5% compared to 2017 Q2. Slightly less dynamic growth was recorded in terms of their total value (approx. 26.2%).

435. In addition, as of 20 June 2018 - i.e. the implementation in Poland of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No. 1093/2010 and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35) - entities willing to provide payment services, e.g. perform money transfers, may apply for the status of a small payment institution (SPI). SPI is an alternative to DPI, much easier to launch, requiring less expenditure, both financial and organisational and legal. The SPI, with some restrictions in terms of amounts and territory, may provide most of the services that were so far reserved for the DPI. Additionally, the SPI may conduct so-called hybrid activity. It means that such an entity may also provide non-financial services. Thus, the SPI licence may be used e.g. for the operation of cryptocurrency stock exchanges, which may generate a higher risk.

[153] It should not be forgotten, however, that many DPIs and OPSs carry out transfers through banks.

Figure No. 8 - Total value of payment transactions executed by DPIs and OPSs (in PLN billion)[154]

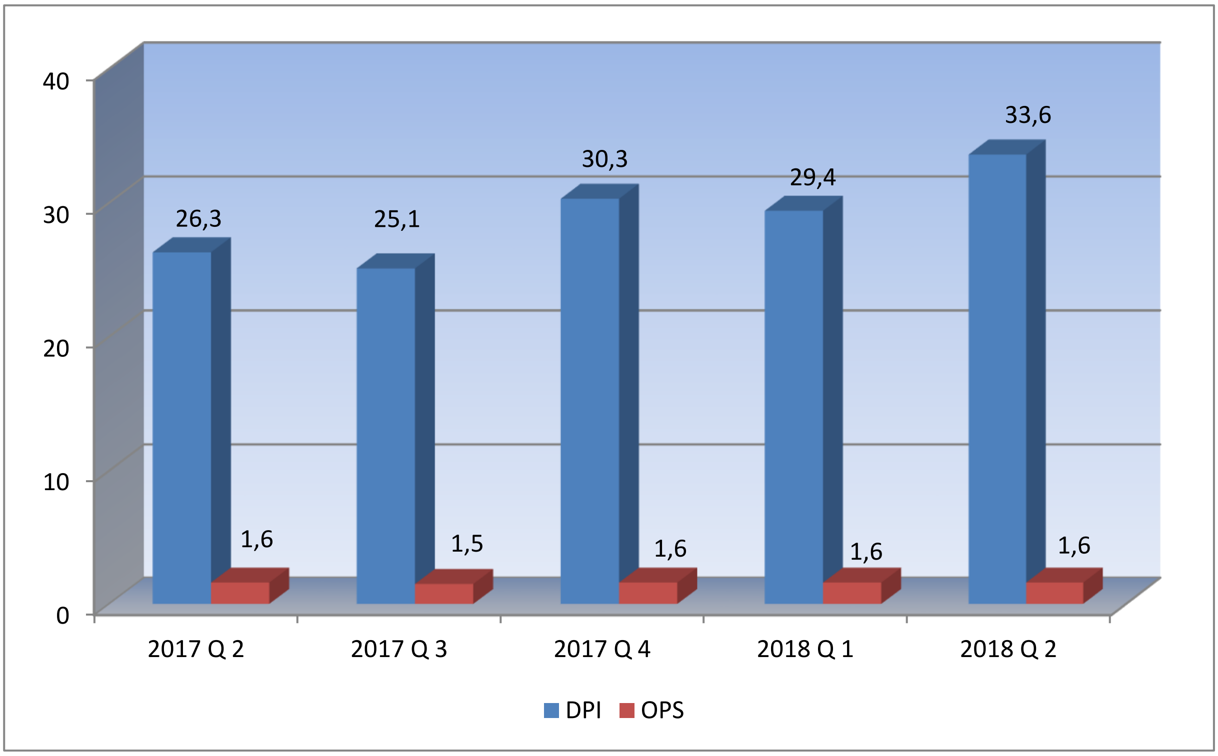
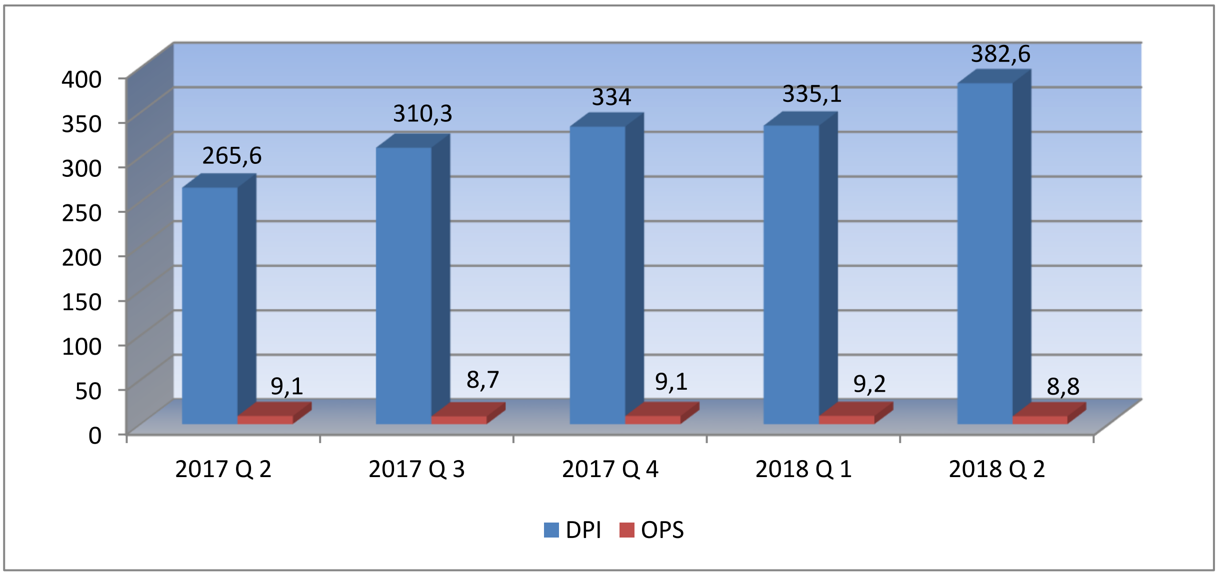


Figure No. 9 - Total Number of payment transactions executed by DPIs and OPSs (in million pcs) [155]



[154] Information on the situation of the DPIs and OPSs in 2018 Q2. Status as of 20 December 2018, Office of the Polish Financial Supervision Authority, Department of Cooperative Savings and Credit Unions and Payment Institutions, Warsaw 2018, p. 4, available at:
https://www.knf.gov.pl/knf/pl/komponenty/img/Informacja_o_sytuacji_KIP_i_BUP_2_Q_2018_64482.pdf.
[155] Ibidem, p. 4.

436. Only DPIs showed growth dynamics. The total value of transactions executed by them in individual quarters systematically increased in the period from the 2017 Q2 to 2018 Q2, while the total value of transactions executed by the OPSs in individual quarters throughout this period remained at a similar level. However, the average value of a single payment transaction at that time remained at a relatively low level, since it amounted to PLN 87.82[156]

437. In accordance with information presented in Figure 7 (entitled: *Analytical proceedings initiated by GIFI in 2016-2018, broken down by products and services used for the execution of suspicious transactions*), only a small part of these proceedings concerned the suspicion of money laundering or financing of terrorism in connection with the use of non-bank payment services for suspicious transactions (in 2016 - about 5.2% of such proceedings and in 2017 - about 1.8%). It can be assumed, however, that this is the result of the fact that payment services offered by banks are much more popular. They give the possibility to execute transactions in different currencies and amounts as well as to combine the use of payment transactions with other products and services offered by banks. Moreover, some banks also act as agencies of payment institutions other than banks or credit institutions.

438. A distinction is usually made between money remittance services, which are mainly based on cash deposits and withdrawals and payment services provided on a non-cash basis with the use of payment accounts (although transactions combining both these types can be executed, e.g. a cash deposit to be transferred on a non-cash basis to the payee's payment account and vice versa).

439. In Poland, money transfer services[157] are offered primarily by OPSs as well as agents of payment service providers established in other EU Member States. Such services are also offered by one of the postal operators. However, it should be noted that an increasing number of entities offering non-bank payment services provide both money remittance and money transfer services[158].

440. There are also entities offering only money transfer services via Internet platforms, often operating outside Poland or the EU. They can be used to transfer money to selected persons and entities, including payments for online purchases or participation in betting and gambling, also offered online. They also enable internal transfers between individual users of a given Internet platform. It happens that foreign entities offering money transfer services via Internet platforms hold accounts with Polish banks, through which they settle transactions ordered by their clients. Thus, the money laundering and financing of terrorism risks associated with their activities are also transferred to those banks that make their accounts available to them.

[156]Ibidem, p. 5.
[157] In accordance with Article 3(3) of the *Act of 19 August 2011 on payment services*, the money remittance service means "a payment service provided without the intermediation of a payment account held for the payer, consisting in the transfer to the payee or to another supplier accepting funds for the payee received from the payer or in the receipt of funds for the payee and making them available to the payee".
[158] In accordance with the definition set out in Article 3(9) of *Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006*, transfer of funds shall mean "any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same....".

441. The risk of using non-bank payment services for money laundering is mainly related to their following characteristics:

- short time of payment transaction execution;
- possibility of executing cross-border transactions between the principal and the payee staying in different countries;
- easy access method - to use payment transactions it is not necessary to hold a bank account, credit cards, cheques (and in the case of money orders - also other payment accounts);
- fast access in the case of payment services offered by Internet platforms (7 days a week from any place worldwide);
- possibility of making transfers of payment services between individual users of a given Internet platform;
- lack of a proper warranty for the application of the anti-money laundering and counter-financing of terrorism principles, due to low opportunity costs resulting from reputation loss;
- lack of control over foreign payment service providers, in particular Internet platforms offering payment services operating outside the EU (limited possibilities to gain access to information on their transactions and the identity of the actual principal and beneficiary of the transfer).

442. Moreover, there is also a risk related to offering of payment services by entities operating illegally, e.g. by using payment accounts maintained for their benefit for the purpose of this activity. This threat is related, among others, to the activity of informal cash transfer systems such as *Hawala*[159]. Their services are frequently used by immigrants who use them to transfer their earnings to relatives in their countries of origin (usually at a lower cost than in the case of regulated payment service providers). Typically, such a system consists of a network of interlinked intermediaries (so-called *hawaladars)* who settle the transactions ordered by their clients between each other by means of the settlement of balances.[160] Services of this type may also be used to transfer funds originating from crime. One of the examples confirming this is the detection in Germany of an Iraqi criminal group (broken up in 2016) involved in money laundering for international drug dealers, among others, through the *Hawala* system[161]

---

[159] In this case, these are the so-called *criminal hawala*described in: FATF report - The role of Hawala and other similar service providers in money laundering and terrorist financing, FATF, October 2013. (at: https://www.fatf-gafi.org/documents/documents/role-hawalas-in-ml-tf.html).

[160] More on this subject in: Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 74-76 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[161]https://www.europol.europa.eu/newsroom/news/iraqi-money-laundering-syndicate-based-in-germany-dismantled-support-europol-and-eurojust, date of reading 13 June 2019.

Currency exchange

443. Currency exchange is not a complicated service, although it can be carried out in several different ways. The basic one consists in cash purchase and sale of convertible currencies and it is most often carried out by entrepreneurs pursuing bureaux de change activities.

444. Bureaux de change activities in Poland are characterised by the fact that most of the transactions performed are occasional, i.e. they not carried out in the framework of business relations.

445. Occasional transactions may be:

- registered transactions - a proof of purchase/sale is issued to confirm the transaction, containing the customer's identification data (name, surname or name of the entity performing the transaction and the place of residence or registered office of the entity performing the transaction as well as the characteristics of the identity document of the person performing the transaction);
- bearer transactions (anonymous transaction) - to confirm the performed transaction, a proof of purchase/sale is issued which does not include data identifying the customer.

446. Occasionally, in the framework of bureaux de change activities, transactions performed in the framework of business relations between an entrepreneur pursuing the bureaux de change activities and the customer are concluded.

447. The risk of money laundering and financing of terrorism associated with such services is mainly affected by the anonymous nature of occasional transactions, often executed below the EUR 15,000 equivalent threshold and the cash nature of the services offered.

448. Risk areas in bureaux de change activities:

1) Customer risk.

- Risk related to servicing a large number of customers

  An increased money laundering and financing of terrorism risk occurs in the case of anonymous transactions conducted in points used by a large number of random customers. This applies to bureaux de change offices located in shopping centres in large cities or tourist centres.

- Risk of disintegrated transactions

  The obligation to inform the GIFI about executed transactions in amounts exceeding the equivalent of EUR 15,000 may be circumvented by carrying out smaller transactions spread over time. Such a risk increases in the case of a large number of bureaux de change located close to each other, e.g. in a single street or square.

- Risk of diverting funds from the country

  The risk of money laundering and financing of terrorism increases in bureaux de change allowing, due to their location, for easy and fast export of foreign currency values abroad. This risk applies both to bureaux de change offices located near the border, in duty-free zones, at airports or railway stations.

2) Risks related to an entrepreneur running a bureaux de change activity.

- Risk arising from an employee's negligence or dishonesty

  Failure to exercise due diligence in complying with the obligations imposed by *the Act of 1 March 2018 on the counteracting money laundering and financing of terrorism*, in particular those related to the application of customer due diligence measures.

- Risk of mixing profits from legal and illegal sources

  Bureaux de change activities may be conducted by a natural person or a legal person and a company without legal personality, which must meet a relatively low level of requirements. There is a risk that such entities may be used to introduce funds originating from crime into financial circulation. The cash nature of the services they offer is conducive to the mixing of legal and illegal profits.

- Risk of anonymous transfer of assets to the benefit of third parties

  Entrepreneurs offering, in addition to bureaux de change activities, additional services of transferring funds to third party foreign exchange accounts or transferring other foreign currency values (e.g. foreign exchange gold) to third parties via mail or via any other intermediary offering parcel delivery services generate the risk associated with the lack of possibility to determine the beneficial owner of the transaction performed by such entrepreneur.

449. In addition to foreign exchange services in cash, cashless foreign exchange services are also offered. They provide a possibility to perform transactions, often at more favourable rates than in the case of cash exchange. Such services are offered both by entrepreneurs pursuing bureaux de change activities[162], banks or financial institutions as well as by other entities. Internet platforms that provide access to them are usually divided into so-called online bureaux de change offices and social currency exchange platforms.

450. In the case of Internet bureaux de change activities, cashless currency exchange is usually carried out according to a similar scheme:

- acceptance by the customer of the terms and conditions of the transaction, in particular the exchange rate offered by the service provider;
- transfer of funds in one currency by the customer to the bank or payment account of the service provider;
- the return transfer of the exchanged funds in another currency by the service provider to a bank or payment account indicated by the customer.

451. Social currency exchange platforms match the foreign currency buy and sell offers submitted by individual clients. In this way, they enable them to perform exchange transactions between them. However, cash flow takes place between the payment accounts of individual customers.

452. In the network it is also possible to find so-called platforms for group currency purchases. Such platforms, on the other hand, offer a possibility to buy currencies at preferential rates used

[162] Cashless currency exchange via the Internet offered by entities pursuing bureaux de change activities is not a bureaux de change activity within the meaning of *the Act of 27 July 2002 - Foreign exchange law* and is carried out outside this activity.

on the foreign currency market. The platform is used to collect orders to buy a given currency from many of its users. The collected orders provide the basis for the execution of one aggregate transaction on the foreign exchange market. This allows for the exchange of foreign currency at a more favourable rate than in the case of ordinary, "retail" transactions.

453. Sometimes, in the case of services offered by entrepreneurs pursuing bureaux de change activities, cash exchange is combined with cashless foreign currency exchange. An illustration of this may be a situation where the customer transfers cash to the service provider for exchange with an instruction to transfer the money to the bank account indicated by the customer. There may also be transactions where the customer transfers money to the service provider for exchange to its bank account and receives the exchanged money in cash[163]. Moreover, payment cards may be used to transfer money for exchange.

454. The risks listed above relating to the activities of entrepreneurs pursuing bureaux de change activity also apply to non-cash foreign exchange services, including the risk of anonymous transfers of assets to third parties (e.g. through designation by the customer as its bank account or other third party payment account to which the service provider should transfer the funds).

455. It is also worth noting that operators of Internet platforms for cashless currency exchange sometimes offer additional services, such as buying and selling virtual currencies or trading on the Forex market.

Virtual currencies

456. The development of products and services that can compete with traditional financial products and services also takes place outside the relevant financial market. A favourable field for their development was created by the rapid progress of information technologies, as well as the progressive computerisation of the society and the development of Internet access networks.

457. In accordance with the FATF report[164], a virtual currency is a “digital representation of value that can be digitally traded and which functions as (1) a means of exchange; and/or (2) a settlement unit; and/or (3) a value resource, but which has no legal tender status [...] in any jurisdiction. It is not issued or guaranteed by any jurisdiction and performs the above functions only under the agreement within the community of users of such virtual currency.”

458. This definition, although it directly indicates that virtual currencies are not a legal tender and indirectly that they do not represent electronic money[165], does not prejudge the legal nature of virtual currencies. Nor does it indicate whether the virtual currency is a commodity, a service or a property right[166].

[163] In the case of bureaux de change activities, transactions with the use of bank accounts shall be permitted only in respect of domestic currency settlements on account of foreign currency cash exchange at a bureaux de change office.
[164] FATF Report - Virtual Currencies Key Definitions and Potential AML/CFT Risks, FATF, June 2014, p. 4.
[165] Through the assumed classification that the notion of virtual currency is included next to the notion of electronic money in the broader term of digital currency - FATF Report - Virtual Currencies Key Definitions and Potential AML/CFT Risks, FATF, June 2014, p. 4.
[166] It is sometimes pointed out that virtual currencies are intangible assets, being a property within the meaning of the Civil Code - see: Virtual Currencies, Wardyński i Wspólnicy, July 2014, p. 18 (available at: http://www.wardynski.com.pl/download/gfx/wardynski/pl/defaultaktualnosci/26/373/1/raport_o_wirtualnych_walutach.pdf).

459. Recently, the FATF has also started to use the term "virtual assets" (understood more broadly than "virtual currencies"). It has been defined as a digital representation of a value that can be traded, transferred and used for payment or investment purposes. However, this concept does not cover the digital representation of legal tender, securities and other financial assets which are already otherwise covered by FATF recommendations. Virtual assets were referred to in FATF Recommendation No. 15, updated in 2018[167].

460. The FATF divided the virtual currencies into:

- centralised currencies (i.e. issued by a single entity) and decentralised currencies (issued using mathematical, cryptographically secured algorithms and without a single publisher controlling the issuing system);
- convertible currencies (i.e. currencies with an equivalent value in one legal tender and which can be exchanged for this and another legal tender) and non-convertible currencies (mainly used in specific virtual environments, e.g. computer games and not exchangeable for legal tender).

461. The notion of virtual currencies is defined under the Polish law in Article 2(2)(26) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in a manner similar to that adopted by the FATF. According to this definition, a virtual currency is a digital representation of the value that is not:

- a legal tender issued by the NBP, foreign central banks or other public administration bodies;
- an international unit of account established by an international organisation and accepted by individual countries belonging to this organisation or cooperating with it;
- electronic money within the meaning of *the Act of 19 August 2011 on Payment Services;*
- a financial instrument within the meaning of *the Act of 29 July 2005 on Trading in Financial Instruments*;
- a bill of exchange or a cheque

– and which is exchangeable in business transactions to legal tender and accepted as the means of exchange as well as can be electronically stored or transferred, or can be subject to electronic trade.

462. Decentralised virtual currencies are often identified as cryptocurrencies, issued on the basis of cryptographic algorithms as part of so-called *distributed ledger technology (DLT*) developed on the basis of *Blockchain* technology which forms the basis for the source code of the first cryptocurrency called Bitcoin (BTC) as well as subsequent alternative cryptocurrencies, the so-called *altcoins*. Another example of DLT technology used for cryptocurrency creation and transaction execution with their use is DAG technology (*Directed Acyclic Graph*), on which the so-called *Tangle* is based which provides grounds for the cryptocurrency called IOTA. The Tangle was created for the implementation of the so-called micropayments within the Internet

[167] International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated in October 2018, p. 15 and 124 (available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html).

of Things (IoT)[168]. Its structure is not based on blocks of transactions linked in chains but on a stream of individual transactions linked to each other.

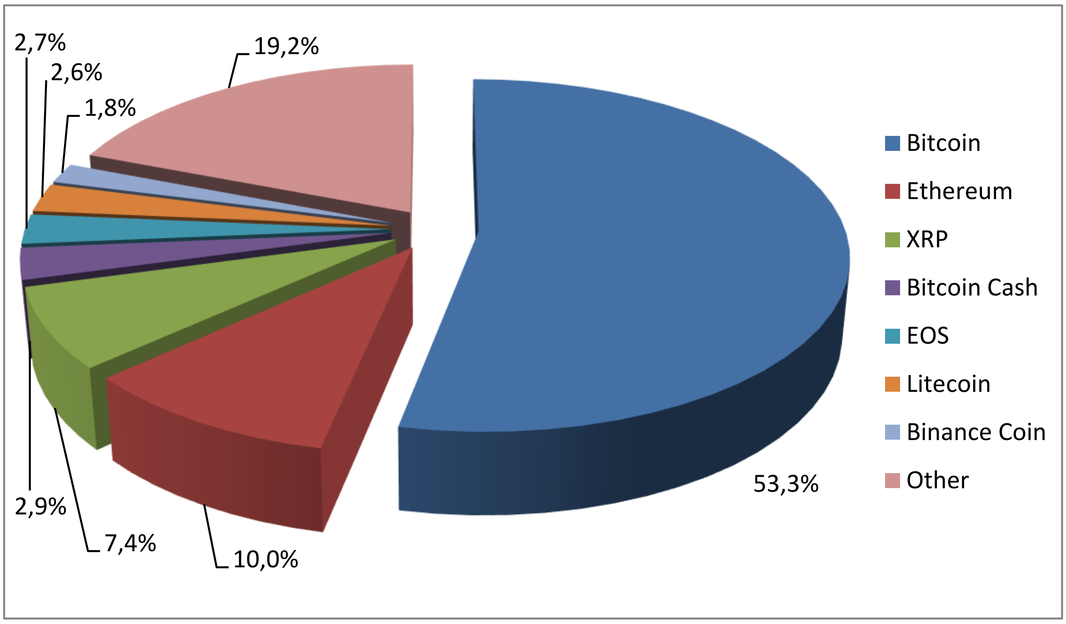
463. In accordance with information from the *coinmarketcap.com* service, as of 23 April 2019, 2132 cryptocurrencies (both *coins* and *tokens*[169]) were available, most of which were *tokens* (approx. 60.3%). Due to the different form of source codes and the saved functionality of each cryptocurrency, each of them may generate different risks for the security of financial transactions. First of all, attention should be paid to cryptocurrencies that guarantee full anonymity, among which such cryptocurrencies as: Z-cash (ZEC) and Monero (XMR), are very popular and many others. In the transaction code, they transmit only the transfer amount, while encrypting other information about the transaction, which allows to ensure full anonymity of the payer and the payee.

464. The analysis of data regarding their capitalisation presented by *coinmarketcap.com* shows that Bitcoin still has the largest share in this market (approx. 53.3%). On the other hand, the 7th place in terms of capitalisation was occupied by *a token* based on solutions of the Ethereum development platform - Binance Coin (BNB), with about 1.8% share in the total capitalisation of cryptocurrencies, which is a settlement means on the cryptocurrency exchange platform *binance.com*.

[168] The first information has already appeared indicating that criminals have found the possibility of using cryptocurrencies based on the DAG technology. According to Europol information of 28 June 2018, one major operation by the Spanish *Guardia Civil* and the Austrian Federal Police, supported by Europol, which aimed to break up a criminal group involved in the production and distribution of synthetic drugs in Darknet and money laundering, property of considerable value was seized (equivalent to at least EUR 12 million). Among others, virtual currencies, but not only Bitcoins (worth over EUR 5.5 million), but also IOTA units (worth EUR 137 thousand) and lumens (worth EUR 30 thousand) - https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe’s-biggest-ever-lsd-bustaccess 30 August 2018

[169] In accordance with the explanation posted on the coinmarketcap.com portal (date of reading - 23 April 2019), the difference between them is based on the fact that *the coin* is a cryptocurrency functioning independently of other cryptocurrencies, whereas the *token* is a cryptocurrency dependent on another cryptocurrency, which is a platform for its functioning.

Chart no. 10 - The percentage share of individual cryptocurrencies in the whole market of cryptocurrency according to the data concerning their capitalisation provided by the coinmaketcap.com service (as of 23 April 2019).



465. The Polish market has proved to be a susceptible ground for the development of activities related to the new type of product. One of the oldest cryptocurrency exchanges in the world - Bitcurex[170] started its operations in Poland in 2012. On the other hand, in 2014, one of the Polish "mines" of virtual currencies was the fifth largest in the world in terms of computing capacity. It should also be noted that according to 2017 estimates, Bitcoin was accepted in Poland by about 130 retail and service outlets. A number of Internet portals also enable buying services or products for cryptocurrencies, e.g. one of the social financing platforms provides its customers with services to sell their shares e.g. for Bitcoins, indicating that "any Bitcoin holder can become a shareholder in your company from anywhere in the world".[171]

466. Information from the website https://gieldykryptowalut.pl/najwieksze-gieldy-i-kantory-kryptowalut/ (dated 15 March 2019) as well as from the websites of the entities mentioned therein and the UKNF (PFSA office) indicates that 19 bureaux de change offices and cryptocurrency exchanges offered their services in Polish on the web, of which 2 entities have an entry in the register of small payment institutions kept by the KNF (PFSA)[172]. However, only 9 of them are operated by entities registered in Poland, others are owned by entities registered mainly in the United Kingdom (in 6 cases). In 2018 and in January 2019, several virtual currency exchanges in Poland closed their operations or moved them to the UK or Malta

[170] Since 2016, the Regional Prosecutor's Office in Łódź has been conducting preparatory proceedings in the case of "leading to unfavourable disposition of property of still unknown number of natural and legal persons in connection with the operations of the Bitcurex exchange run by "Digital Future Spółka z ograniczoną odpowiedzialnością" Spółka komandytowa with its registered office in Łódź" http://www.lodz.po.gov.pl/pliki/2017/k/20170217_K2.pdf, access 6 September 2018).
[171] https://beesfund.com/pomoc , date of reading 8 May 2019
[172] Source: KNF (PFSA) register of small payment institutions and articles available at the following links: https://www.cashless.pl/5274-bitclude-knf-licencja, https://www.cashless.pl/5282-gielda-kryptowalut-coinquista-knf.

after they had been included in the KNF (PFSA) warning list but it is estimated that around 75% of their clients are still Polish clients.

467. The distinction between exchanges and crypto-currency bureaux de change is based on the difference in their business models. Crypto-currency bureaux de change provide their services both on the Internet and in stationary service points. They enable their customers to buy or sell a certain amount of decentralised virtual currency units. They do not offer storage services for these units or private keys to access them.

468. On the other hand, crypto currency exchanges provide a wider range of services. Buy and sell transactions of cryptocurrency units can be concluded with the cryptocurrency exchange, as well as on the basis of matching buy and sell offers of its clients - between their different users. In addition, they offer their clients managing electronic portfolios on their behalf. Owing to these wallets (also known as "hot wallets"), the client can submit an order at any time, e.g. exchange of legal tender into virtual currency or transfer of resources held to another portfolio, including an over-the-counter portfolio (e.g. own *off-line* portfolio - the so-called "cold wallet").

469. In addition to the possibility to buy or sell decentralised units of virtual currencies, cryptocurrency exchanges provide access to a wide range of different market information - the values of individual virtual currencies, volumes and trends.

470. Statistical data concerning the activity of one of the cryptocurrency exchanges shows that in one month of 2018 its customers carried out nearly 5 thousand cryptocurrency purchase transactions. The arithmetic mean value of a transaction was about PLN 755.00 and the median - PLN 230.00. The above indicates that the value of most of the transactions executed on this exchange is relatively low.

471. In Poland, it is also possible to buy and sell decentralised virtual currencies for cash, either at stationary points of some exchanges and cryptocurrency bureaux de change offices or through dedicated ATMs, so-called bitmats. According to the information provided by https://coinatmradar.com/ service, as of 15 March 2019, 36 machines operated in Poland, thanks to which it was possible to buy or sell Bitcoins or other virtual currencies (Bitcoin Cash, Litecoin, Dash, Ether). The growing network of bitmats in Poland, a considerable anonymity provided by virtual currencies and splitting of transactions into smaller amounts enable money laundering and its transfer abroad or from abroad to Poland, outside the banking system.

472. Contrary to legal tender, decentralised virtual currencies have no equivalent in the form of banknotes and coins and are not subject to control by the central bank or other public authorities (lack of supervision and financial guarantee by the State). Moreover, the possibilities to hide the identity of their users, as well as the tools to mix and tangle transactions in order to complicate the links between them and their users[173] are well developed. This contributes to reducing the traceability of cash flows and the verification of data concerning their holders. Consequently, criminals (in particular those operating in cyberspace) show an increasing interest in them. For this reason, they are used, inter alia, as a means of payment of ransom for extortion in cyberspace as well as in trade in illicit goods (e.g. drugs, firearms, forged or counterfeit documents or information obtained illegally) or services.

[173] So-called *anonymisers* - i.e. *tumblers, mixers*.

473. In addition to decentralised virtual currencies, centralised virtual currencies are also available. They include, among others, *WebMoney* or *PerfectMoney*, i.e. virtual currencies used by some entities to offer payment services (as a digital representation of the values collected by the customers of such entities in their electronic portfolios as well as the object of transactions performed between them). The value of units of most types of *WebMoney* and *PerfectMoney* is closely related to the value of the specific legal tender (e.g. US dollars, roubles). However, there are also some currencies with the value related to the Bitcoin or gold exchange rate.

474. The practice and experience of law enforcement authorities shows that the risk related to the use of cryptocurrencies for criminal activities, including: money laundering[174], fraud, in particular committed with the use of ICT networks, in settlements related to extortion resulting from "ransomware" type attacks, is growing[175]. An equally important and predictable threat is the possibility for criminals to use cryptocurrency to eliminate the risk of seizure by law enforcement authorities of illegally obtained financial gains. The source of this threat is primarily the fact that money laundering through trading in virtual currencies can be easily carried out on an international scale due to the global functioning of such virtual currencies, easy access to services in the scope of their exchange from/to cash and the relatively high anonymity of their users[176]

475. Another problem is that criminal groups are exploiting trends associated with the growth in the value of virtual currencies and offering the purchase of such assets[177] on the financial market, making this activity dependent on the payment of funds to bank accounts belonging to companies set up specifically for this purpose. These behaviours are fraudulent to the detriment of retail investors.

476. Analytical proceedings conducted in 2016-2018 by the GIFI also included those concerning the suspicion of money laundering while using, among others, virtual currencies. They were related, inter alia, to suspected criminal activities such as hacker attacks, fraud (including tax fraud), financial pyramid schemes, illicit trafficking in psychoactive substances, including drugs.

---

[174] One of the examples was indicated on the CBŚP website. It was related to an investigation into the fraud involving 17 fictitious online shops offering electronic equipment and household appliances. The money obtained was transferred by criminals to the cryptocurrency exchanges in Poland and abroad (see: http://cbsp.policja.pl/cbs/aktualnosci/160217,Mogli-oszukac-nawet-2700-osob.htmlread on 23 April 2019).
Another example is described on the website of the District Prosecutor's Office in Jelenia Góra. It was related to an investigation concerning a criminal group which fraudulently sold vehicles on web portals. A part of the acquired funds was invested in cryptocurrency. The prosecutor’s office secured, among others, eight Bitcoins. "Pursuant to the prosecutor’s order, on 22 March 2018, the Head of the Tax Office in Lubań sold the secured cryptocurrency, acquiring the amount of PLN 237,137.80.” (see: https://jgora.po.gov.pl/komunikat-prasowy-nr-192018,new,mg,306.html,63 , read: 23 April 2019).

[175] Hacker attacks using malicious software encrypting files on a computer in order to force a ransom for their decryption.

[176] One of the examples of detecting such a practice may be the case from 2018, concerning seizing by the National Prosecutor's Office and the CBŚP of nearly PLN 1.3 billion, which was suspected to have come from money laundering from drug business, probably with the use of cryptocurrencies (see: https://www.pap.pl/aktualnosci/news,1360200,ziobro-zabezpieczono-blisko-13-mld-zl-z-narkobiznesu.html).

[177] An example are virtual currencies such as *Dascoin* or *Onecoin* (which are not, however, cryptocurrencies). The creators of Onecoin were arrested by the US authorities in March 2019 on suspicion of creating a financial pyramid (see: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-leaders-onecoin-multibillion-dollar#_ftn2).

477. Following the *Communication of the National Bank of Poland and the Polish Financial Supervision Authority on virtual "currencies*" of 7 July 2017, risks related to the use of virtual currencies can be mentioned as examples of risks related to the use of virtual currencies:

- the risk of losing funds caused by theft due to the fact that virtual currencies may be stolen, e.g. as a result of a cyberattack on a virtual currency trader or user infrastructure;
- the risk related to the lack of guarantees (funds held in virtual currencies are not guaranteed by the Bank Guarantee Fund since they are not bank deposits);
- the risk related to the lack of universal acceptability (they are not a legal tender and are therefore not widely accepted in business transactions, only a small part of retail outlets accepts them);
- the risk related to the possibility of fraud (some of the offered forms of investing in virtual currencies may be financial pyramid-like, which - additionally, due to the specific risks described above - may lead to the loss of the investor's financial resources in a short period of time);
- the risk associated with considerable price volatility (e.g. changes in the exchange rate of the best known decentralised virtual currency, Bitcoin, at the turn of 2017 and 2018).

478. The risks associated with virtual currencies are also affected by the concentration of ownership of some virtual currencies, which facilitates manipulation of their value. According to data provided by Credit Suisse analysts in January 2018, 97% of Bitcoins are held in just 4% of all virtual wallets[178].

479. It is worth noting the ease of transferring significant property values in the form of cryptocurrencies on digital media, such as Trezor or Ledger Nano S, which can approve the record of an infinite amount of a given cryptocurrency in the form of the so-called "cold wallet".

480. Additionally, it is worth noting the possibility of using the DLT technology to raise funds for various purposes. The so-called initial coin offerings (ICO) simply represent another form of acquiring financing for various types of projects, including those undertaken in the scope of *FinTech.* This process usually takes place by issuing a new *token* through a public *blockchain*, which is then acquired by interested investors usually for commonly exchangeable *coins*, e.g. Bitcoins. For this purpose, for example, ETHEREUM[179] and OMNI[180]platforms can be used. ICOs are usually advertised on various internet fora, e.g. *Bitcointalk*.

[178] Charles Brennan, Brad Zelnick, Mathew Yates and William Lunn, Blockchain 2.0, ed. Credit Suisse, 11 January 2018, p. 19 (available at: https://research-doc.credit-suisse.com).
[179] In accordance with the information provided on the website https://www.ethereum.org/crowdsale (access on 12 October 2018): "Instead we are going to do this the decentralized way and just create a token to keep track of rewards, anyone who contributes gets a token that they can trade, sell or keep for later. When the time comes to give the physical reward the producer only needs to exchange the tokens for real products. Donors get to keep their tokens, even if the project doesn't achieve its goals, as a souvenir".
[180] In accordance with the information provided on the website https://www.omnilayer.org/#About (access on 12 October 2018): "Decentralized crowdfunding is easy with Omni. Crowdsale participants can send bitcoins or tokens directly to an issuer address and the Omni Layer automatically delivers the crowdfunded tokens to the sender in return - all without needing to trust a third party".

481. The ICOs can also be used for criminal purposes, e.g. for fraud and the extortion of property values through misleading in relation to projects which should be financed or possible returns on investment, including the creation of financial pyramid schemes of various kinds. This is fostered by, inter alia, the lack of legal regulations in this area, frequent lack of complete information on the project or the possibility of its verification as well as limited possibilities of withdrawing from the project investment (related in particular to the non-convertibility of *tokens* acquired for the property values and dependence on their issuers in this respect).

482. The risk of ICOs being used for money laundering or financing of terrorism is associated with their characteristic features, such as:

- lack of transparency in the use of collected funds;
- cross-border nature of transactions executed (gathering of assets from entities from different parts of the world);
- the ease of using the "straw men" or fictitious personal data to legalise property values originating from crime invested in real or specially designed projects.

483. It is worth noting that some public authorities from various countries issued warnings concerning the risks associated with the ICO. Among others, a similar warning was issued by the KNF (PFSA) in November 2017[181]

484. The degree of technological advancement of virtual currencies may complicate the analysis of transactions, examining the source of property values and the use of suspending a transaction or blocking an account in the case of suspicion of money laundering or financing of terrorism. It should also be noted that due to their characteristics, virtual currencies (mainly cryptocurrencies) may also hinder the application of specific restrictive measures.

FOREX

485. In accordance with the definition presented by the KNF (PFSA), the FOREX market (also referred to as the OTC derivatives market) is "the area of the capital market, over-the-counter, where transactions are concluded, especially via Internet trading platforms, addressed to derivatives, in particular contracts for differences and options"[182].

486. Services in this scope are offered by both domestic and foreign entities. In the case of domestic entities, these are brokerage houses and banks (it can be both a bank with a brokerage license and a “standard” bank operating under the provisions of *the Act* of *29 August 1997. - Banking law*).

487. Polish residents also have access to the offer of foreign entities, often via the Internet. Pursuant to the law, such an offer may be provided by foreign investment firms conducting brokerage activities in Poland through a branch or on a cross-border basis - without the need to open it, which have their registered offices in the territory of the European Union or the

[181] KNF (PFSA) Communication concerning the sale of so-called coins or tokens Initial Token Offerings (ITOs or Initial Coin Offerings (ICOs)), KNF (PFSA), 22 November 2017, available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_ICO.pdf.

[182] Maciej Kurzajewski and Dorota Nowalińska, Profit and risk on the FOREX market. Financial service client’s guide, KNF (PFSA), Warsaw 2017, p. 7 (available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Zysk_a_ryzyko_na_rynku_Forex_59289.pdf).

European Economic Area and have notified that they carry out such activities or have the appropriate KNF (PFSA) licence.

488. Some of the aforementioned entities do not appear in the advertising content under actual, registered names, but use other trade names (brands) for this purpose. It is also not uncommon for one entity to use more than one trade name or to change brands relatively frequently[183]

489. In April 2017, the KNF (PFSA) issued an announcement in which it emphasised the risk related to the occurrence of so-called price slippage in transactions concluded on "forex trading platforms"[184]. It describes these risks in terms of the mode of execution of client orders by investment firms operating in the *market maker* model (although it is noted that they may also refer to orders placed through firms other than operating in this model which, however, submit orders for execution to a trading platform that operates in this way).

490. Investing in the FOREX market is risky. While trading on it, investors hope to make a profit from increases in exchange rates, commodities, stocks and goods or decreases in exchange rates. However, these transactions are largely speculative because "...the Forex market is difficult to predict for an individual and inexperienced trader, especially when the other party to the transaction is a Forex broker who controls all the data on its trading platform and has knowledge concerning the orders of all his clients"[185]

491. In accordance with the KNF (PFSA) announcement of 25 April 2017 regarding the results achieved by investors on the FOREX market in 2016, as many as approx. 79.3% of active clients using FOREX online trading platforms suffered losses (the analysis was based on information from domestic brokers offering such services to their clients)[186]. It was also noted that "...the results of brokerage houses' clients obtained on particular classes of derivatives in short time horizons (quarterly cycles) indicate a higher percentage of clients achieving profit, in a longer time horizon, about 80% of clients performing transactions on the Forex market ultimately incur a loss" while the survey conducted by the UKNF (PFSA office) "on the results of clients on the Forex market in the years 2012-2016 indicate that this ratio remains at a similar level and is close to the results of surveys conducted by other supervisory authorities from the European Union".

492. In its analytical report of 2016, the CBA drew attention to the risks related to the activity of the FOREX market which focus on 4 issues:

- conflicts of interest (in particular, in relation to brokers operating in the *market maker* model);
- investment risk (resulting primarily from considerable fluctuations in currency exchange rates as well as from the structure and nature of the FOREX market) and

---

[183] Ibidem, p. 8.

[184] Communication on the risks related to the occurrence of so-called price slippages in the process of execution of client orders by investment firms on the Forex market, KNF (PFSA), 25 April 2017, available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_Slippage_forex_25_04_2017_55678.pdf.

[185] Maciej Kurzajewski and Dorota Nowalińska, Profit and risk on the FOREX market. Financial service client's guide, KNF (PFSA), Warsaw 2017, p. 22 (available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Zysk%20a%20ryzyko%20na%20rynku%20Forex_59289.pdf)..

[186] Announcement concerning the results achieved by investors on the FOREX market, KNF (PFSA), 25 April 2017, KNF (PFSA), available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_wyniki_klientow_forex_25_04_2017.pdf.

commission risk (the level of which also affects the potential results of customers' investments);

- ICT platforms (whose functioning is related to the risk of susceptibility to computer crime);
- licensing and supervision (treating high-risk derivatives specific to FOREX as other derivatives as well as the operation of brokers offering such services online without appropriate authorisation and control)[187].

493. The FOREX market and transactions concluded on it may be used to commit basic crimes for money laundering. This may include fraud based on misleading customers[188] (e.g. by providing false expert opinions or financial analyses) or favouring certain customers (e.g. by providing them with confidential information about others' orders), computer crime (e.g. related to unauthorised access to customer accounts) as well as corruption offences.

494. As in the case of other financial institutions, there is also a possibility to use the FOREX market for money laundering, in particular when the broker is controlled by criminals and orders are placed by criminals or persons substituting them.

Securities

495. Pursuant to Article 3(1) of *the Act of 29 July 2005 on trading in financial instruments*, securities shall mean:

a) shares, pre-emptive rights within the meaning of *the Act of 15 September 2000 - Commercial Companies Code*, rights to shares, subscription warrants, depository receipts, bonds, mortgage bonds, investment certificates and other transferable securities, including property rights incorporating property rights corresponding to rights arising from shares or from debt assumption, issued under relevant provisions of Polish or foreign law;

b) other negotiable property rights which arise from an issue, incorporating the right to acquire or subscribe for the securities referred to in subparagraph (a) or exercised by cash settlement, relating to the securities referred to in subparagraph (a), currencies, interest rates, yields, commodities and other indicators or measures (derivative rights).

496. Securities may be traded within organised trading or over-the-counter.

497. Although Figure 7 (entitled *Completed analytical proceedings instituted by GIFI in 2016-2018, broken down by products and services used for execution of suspicious transactions*) shows that only a small part of analytical proceedings initiated and completed by GIFI in the years 2016-2018 involved capital market instruments (i.e. not only securities, but also other

[187] Threats related to the functioning of the FOREX market, Analytical Report, CBA Analysis Department, Warsaw 2016, pp. 3-8.

[188] See: https://pk.gov.pl/aktualnosci/aktualnosci-z-kraju/zatrzymania-i-zarzuty-w-zwiazku-z-inwestowaniem-srodkow-finansowych-na-rynku-forex/, https://pk.gov.pl/aktualnosci/aktualnosci-z-kraju/zarzuty-dla-kolejnych-czlonkow-zorganizowanej-grupy-przestepczej-dokonujacej-oszustw-na-rynku-forex/, https://pk.gov.pl/aktualnosci/aktualnosci-z-kraju/kolejne-zatrzymania-w-zwiazku-z-oszustwami-na-rynku-forex/, date of reading 18 June 2019

financial instruments, including derivatives), this does not mean that the risk of their use for money laundering is low.[189]

498. Securities and related products and services can be used for money laundering in different ways. In the guide for obligated institutions and cooperating units entitled "Counteracting money laundering and financing of terrorism" (3rd edition, 2009), the GIFI indicated the methods that can be used for money laundering. Among these methods, the basic methods of using trading in securities and other financial instruments between two Contracting Parties were discussed as well as the use of securities and cash accounts to service the former, for this purpose. In particular, the following sources of money laundering risk by means of these products can be mentioned:

- international nature some transactions relating to trading in securities and other financial instruments;
- high liquidity of some securities which enables their relatively easy conversion into cash;
- high price volatility of certain securities which may involve a possibility of price manipulation;
- existence of securities with far-reaching anonymity of their users (e.g. bearer shares in the case of non-public companies);
- trading in certain securities and other financial instruments over-the-counter;
- possibility of transferring securities between different securities accounts;
- existence of omnibus accounts, i.e. securities accounts in which dematerialised securities may be recorded that do not belong to the persons for whom such accounts are held;
- possibility of executing payment transactions using cash accounts to service securities accounts.

499. In particular, attention should be paid to possibilities of trading in shares under private placements.

Trading in registered shares under private placements

Pursuant to Article 339 of the Act of 15 September 2000 - Commercial Companies Code (Journal of Laws of 2019 item 505 as amended): "The transfer of a registered share or a temporary certificate shall be effected by way of a written declaration either on the share certificate itself, or on a temporary certificate or in a separate document and shall require the transfer of the shares or the temporary certificate." In connection with the foregoing provision, the effective transfer of shares does not require the intermediation of a notary, investment firm or other obligated institution. Thus, no one is obliged to apply customer due diligence measures towards the parties to the transaction.

Pursuant to Article 341§1 of the ksh: "The Management Board is bound to keep a book of registered shares and temporary certificates (share register), in which should be entered the first name and surname or the company (name) and the registered office and address of the shareholder or service

[189] In general, since the income from transactions in securities on the capital market has been taxed and an individual PIT-8C is issued for each investor, the attractiveness of this method of money laundering has decreased.

address, the amount of payments made as well as, at the request of an authorised person, an entry on the transfer of shares to another person together with the date of entry." It should be remembered, however, that a joint-stock company does not have any similar obligations towards its shareholders as an obligated institution has towards its clients with respect to the application of customer due diligence measures.

Article 341 § 1 of the ksh provides that at the request of a purchaser of shares or a pledgee or user, the Management Board shall make an entry on the transfer of shares or establishment of a limited right in rem thereon. On the other hand, Article 341 § 5 of the ksh indicates that the applicants referred to in § 2 are bound to submit documents justifying the entry to the company. The Management Board is not obliged to examine the authenticity of the signatures of the seller of the shares or the persons establishing the pledge or use of the shares.

The foregoing implies that only the parties to the agreement, within due diligence, mutually identify and verify their identity. On the other hand, it can be inferred from Article 341 § 5 of ksh that since the Management Board is not obliged to examine the authenticity of signatures of the seller of shares and persons establishing a pledge or use of shares, there is no obligation to identify and verify their identity.

It is also worth remembering that in accordance with the verdict of the Supreme Court of 4 December 2009 III CSK 85/09 (published: OSNC 2010/7-8/113) in the light of Article 343 § 1 of the ksh, an entry in the share register is only valid as evidence. The fulfilment of the prerequisites specified in Article 339 of the ksh or in Article 925 and 926 § 1 of the ksh has an effect not only on the purchaser of registered shares, but also on all third parties, thus also on the company. The entry of the purchaser in the share register does not, therefore, in any way affect the effectiveness of the acquisition of shares vis-à-vis third parties.

Thus, it can be assumed that registered shares can be traded entirely outside obligated institutions, i.e. outside the system for investigating whether they are related to money laundering or financing of terrorism.

Although pursuant to Article 342 of the ksh, a company may commission a bank or investment firm in the Republic of Poland to maintain a share register. It should be borne in mind, however, that a bank or an investment firm, in accordance with the "nemo plus iuris in alium transferre potest quam ipse habet" principle, shall not have any additional rights towards its shareholders. They cannot apply customer due diligence measures to shareholders since the company is a customer of a bank or an investment firm.

If a shareholder submits a request for a change in the share register, there may be a chain of other persons between it and the shareholder currently listed in the share register (example of share transfer: shareholder in the share register → shareholder 2 → shareholder 3 → shareholder 3 → shareholder N → new shareholder applying for an entry in the share register). An indirect consequence of this status is that in certain situations a company can only presume who the beneficial owner is.

Trading in bearer shares under private placements

In the case of transfer of ownership of bearer shares, Article 92[112] of the Civil Code shall apply, pursuant to which the transfer of rights from a document to bearer requires the issuance of such a document. It should be remembered here that the Supreme Court in its verdict of 3 June 2015 (V CSK 566/14) ruled that with respect to bearer shares, the issue of a document is understood not only *as a transfer of shareholding through the physical issue of a document (Article 348 of the Civil Code), but may also take place using other methods of transferring the shareholding (Articles 349-351 of the Civil Code).*

As in the case of bearer shares, these shares may be traded without the participation of obligated institutions, so the same situation occurs here as in the case of the sale of bearer shares.

The change pattern of shareholders may be as follows: shareholder 1 → shareholder 2 → shareholder 2 → shareholder 3 → shareholder 3 → shareholder N → new shareholder wishing to participate in the General Meeting of Shareholders.

In this context, the following risks arise:

- *ensuring that participants in the money laundering process through private equity trading have a certain "comfort at work" in view of the lack of entities that could identify suspicious transactions;*
- *the possibility to use "straw men" or stolen identity in the chain of traders in shares due to the lack of identification and verification of the identity of the parties to the transaction by an external entity;*
- *the possibility of a bribe that is likely to remain undetected due to a failure to verify that one of the parties to the transaction is not a politically exposed person;*
- *the possibility of making payments for shares in cash, which may lead to funds being invested in this way;*
- *the possibility of legitimising money derived from illegal activities under a share purchase agreement for cash (the same agreement presented as a source of cash invested in an obligated institution);*
- *the possibility to legitimise dirty money on the basis of many share purchase agreements for cash (members of a laundering group conclude agreements between themselves, presenting them as a source of cash invested in an obligated institution - the parties to the agreements obviously do not pay for the purchased shares).*

500. Special attention has recently been paid to corporate bonds, i.e. "securities issued by companies to raise capital for their operations", which certify that "the issuer (entrepreneur) has a debt towards the purchaser (investor, bondholder)" and "the purchasers of bonds are entitled to receive interest and return capital at maturity of the bonds"[190]. Information on risks related to them appeared on the website of the Financial Ombudsman[191] and the KNF (PFSA). Among others, the KNF (PFSA) indicated that it "observes an increased number of public and private offers of bonds other than those issued by the State Treasury addressed to individual investors", as well as "a significant interest of investors in this form of capital investment, which results from a higher interest rate of these bonds in relation to the interest rate of bank deposits" and "a significant involvement of banks in offering these instruments to investors"[192].

---

[190] Corporate Bonds, UOKiK, 2 July 2018, available at: https://finanse.uokik.gov.pl/strona-glowna/obligacje.
[191] *See:* Investments in bonds not always safe, Analysis of the Financial Ombudsman, Warsaw, 16 November 2017, available at: https://rf.gov.pl/pdf/Obligacje_rzecznik_analiza_16.11.pdf.
[192] Announcement of the KNF (PFSA) concerning offering of bonds, KNF (PFSA), 29 May 2018, available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_KNF_ws_oferowania_obligacji_61922.pdf.

501. On the primary market, corporate bonds may be offered as part of a public or private placement. At the same time, "the majority of corporate bond issues are carried out in this latter way"[193]. Within the latter, there is more scope for abuse or use of the predicate offence for the purpose of money laundering. This is due to the characteristics of the private placement, such as: the relatively short term, uncomplicated issue process - as compared to to the procedures under a public offer - low formal requirements (e.g. no requirement to prepare a public information document) and a relatively low issue cost. These characteristics as well as the fact that private placement is intended for a selected group of purchasers, may also foster their use for money laundering.

Investment funds

502. On the Internet, it is possible to find a lot of information on the risks related to the functioning of investment funds, however, they usually refer to the broadly understood investment risk. The KNF (PFSA) defines them as the "uncertainty as to the final outcome of the investment. For this reason, an investment fund, both open-end and closed-end, never guarantees the achievement of the investment objective indicated in the fund's Articles of Association. The source of risk may be various macro- and microeconomic factors influencing, directly or indirectly, the market valuation of the fund's assets[194]

503. According to IZFiA information on its website: "In general, the level of investment risk in the case of funds is determined by two factors: the type of fund and the investment strategy pursued. In short periods of time, equity funds are most exposed to fluctuations in the value of participation units, followed by balanced funds. The lowest risk of fluctuations accompanies debt and money funds. On the other hand, potential profits are the lowest possible for the last two groups, while for equity funds they are the highest"[195].

504. Within the framework of general investment risk, it is possible to distinguish - following the information of IZFiA - the risk of exchange trend (concerning mainly equity, mixed and debt funds), the risk of interest rate changes (e.g. increasing the level of interest rates by the Monetary Policy Council raises the cost of financing the activity of enterprises by means of bank loans and thus limits the profits of enterprises, which will have a negative impact on equity funds and the value of participation units) or currency risk (to which primarily customers of investment funds investing abroad are exposed).

505. Moreover, examples of investment risk may also include, among others:

- macroeconomic risk (related to the situation in the particular country where the fund invests);
- market risk (relating to changes in the economic, political or legal environment and general economic conditions in financial markets);

---

[193] Corporate Bond Market in Poland, Special Report, CBA Analysis Department, Warsaw 2018, p. 4.
[194] Agnieszka Siwek, Łukasz Wojakowski, Participation units and investment certificates of investment funds - comparison of legal and organisational issues. Financial service client's guide, KNF (PFSA), Warsaw 2016, p. 11, available at: https://www.knf.gov.pl/?articleId=54141_id=18.
[195] Risk related to investment in investment funds, IZFiA Guide, 13 April 2015, available at: https://szkolenia.izfa.pl/poradnik,25/39,ryzyko-zwiazane-z-inwestycja-w-fundusze-inwestycyjne.html.

- liquidity risk (resulting primarily from potential limitation of the possibility to buy or sell financial instruments in a short period of time without a significant impact on their price);
- inflation risk (inflation as a reason for lowering the real rate of return on investment);
- credit risk (related to the failure of the issuer of a financial instrument to fulfil its obligations arising from issuing of that instrument)[196]

506. In addition, the management quality risk[197] can be distinguished, related to the way the investment funds manage assets entrusted by their clients.

507. When considering the functioning of investment funds in terms of the threat of their use for money laundering, it should first of all be noted that perpetrators may invest the proceeds of crime in investment funds, similar to other financial services. This could be done as part of a wider plan to use the various products and services offered on the financial market, stipulating the use of the purchase transaction and imminent sale of units or investment certificates as one of the intermediate stages of money laundering and as a destination for location of laundered funds. In each of these situations and in particular in the case of the latter, it is likely to be important for the perpetrators to assess the investment risk and a possibility of potential loss of funds entrusted to them.

508. When considering the risk of money laundering and financing of terrorism, special attention should be paid to closed-end investment funds (FIZs) because of their characteristics that may contribute to committing of these crimes. First of all, unlike open-end investment funds, their offer is usually addressed to a narrower circle of participants. In addition, FIZ managers "have greater freedom in asset allocation using a wider spectrum of financial tools, which creates the possibility of developing an investment policy tailored to the preferences of a specific client"[198]. Pursuant to Article 145(1) and (2) of *the Act of 27 May 2004 on investment funds and management of alternative investment funds*, the FIZ may invest funds in the following transferable assets:

- securities;
- receivables (although only FIZs established as securitisation funds or private equity funds[199] may invest in receivables from natural persons);
- shares in limited liability companies;
- currencies:

[196] https://www.pekao.com.pl/private/nasza_oferta/rozwiazania_finansowe/ryzyka_funduszeaccess 20 November 2018.

[197] Agnieszka Siwek, Łukasz Wojakowski, Participation units and investment certificates of investment funds - comparison of legal and organisational issues. Financial service client's guide, KNF (PFSA), Warsaw 2016, p. 12, available at: https://www.knf.gov.pl/?articleId=54141_id=18.

[198] Threats to the economic interest of the state related to the activity of closed-end investment funds, Special Report, Department of Analyses of the CBA, Warsaw 2018, p. 5.

[199] i.e. a private equity fund that invests at least 80% of its assets in assets other than:

- securities being subject to public offering or securities admitted to trading on the regulated market, unless the securities have become the subject to public offering or have been admitted to trading on the regulated market after their purchasing by the Fund,
- financial market instruments unless they have been issued by non-public companies whose stocks or shares are included in the Fund investment portfolio.

- derivatives, including non-standardised derivatives;
- property rights, the price of which depends directly or indirectly on the type of property, specific types of energy, meters and limits of production or emission of pollutants, admitted to trading on commodity exchanges;
- money market instruments.

509. Moreover, the subject of FIZ deposits may also include deposits in domestic banks, foreign banks or credit institutions,[200] ownership or co-ownership of land property within the meaning of the regulations on real estate management, buildings and premises constituting separate real property, sea vessels, as well as perpetual usufruct [201] (Article 147 of *the Act of 27 May 2004 on investment funds and management of alternative investment funds*). However, most of the restrictions concerning the share of the value of particular categories of assets in investment fund deposits indicated in the aforementioned Act do not apply to FIZ.

510. Some evaluations of FIZ activities indicate that they create favourable conditions for tax optimization as well as money laundering[202]. Although the changes in tax regulations in 2016 abolished FIZ exemptions in the scope of corporate income tax as of 1 January 2017, there is still a risk of their use for tax optimisation[203] or money laundering. This is, among others, due to the fact that since 4 December 2011, i.e. the date of entry into force of *the Act of 16 September 2011 amending the Act on investment funds and the Act on corporate income tax* (Journal of Laws No. 234, item 1389), the KNF (PFSA) ceased to license FIZs issuing only investment certificates, other than offered by public offering, admitted to trading on the regulated market or introduced to the alternative trading system.

511. The main source of money laundering risk for FIZs are their following characteristics:

- collection and allocation of funds from a closed circle of natural persons and economic operators;
- wider investment opportunities than in the case of other types of investment funds;
- opportunities to invest in various assets, both domestic and foreign, including those with a high risk of money laundering[204].

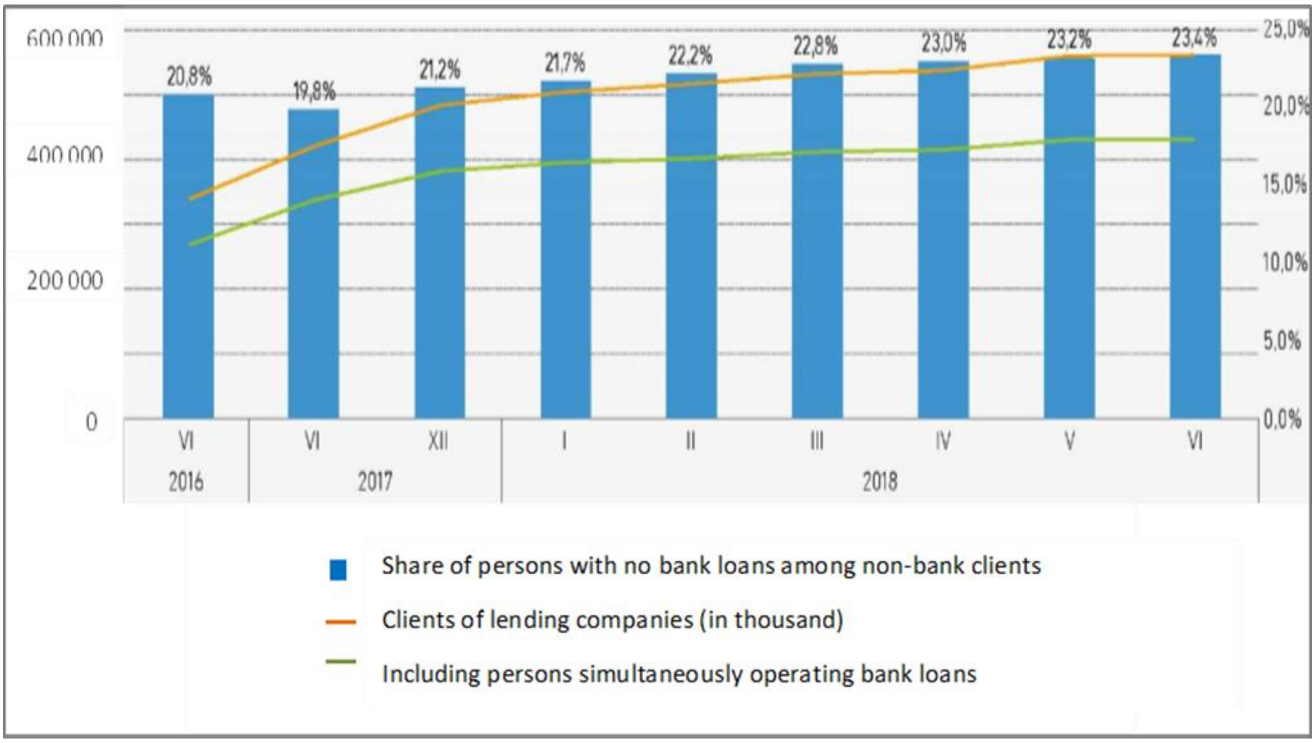
Non-bank loans

512. Loans granted by entities other than banks or SKOK are also used for money laundering. Theoretically, any natural or legal person can be a borrower or lender. The Civil Code regulates the lending rules to a very limited extent.

[200] In accordance with Article 145(7) of *the Act of 27 May 2004 on investment funds and management of alternative investment funds.*
[201] In accordance with the Article 147 of *the Act of 27 May 2004 on investment funds and management of alternative investment funds.*
[202] Some information shows that there are difficulties in identifying the actual beneficiaries of such funds due to the refusal to provide information on the participants of these funds to other obligated institutions intermediating in the implementation of transactions of these funds.
[203] After the new regulations came into force, only the optimisation method was changed (see: Threats to the economic interest of the state related to the activity of closed-end investment funds, Special Report, Department of Analyses of the CBA, Warsaw 2018, p. 8-9.
[204]Ibidem, p. 9.

513. The development of the non-banking sector in the scope of lending is more and more visible. The report of Biuro Informacji Kredytowej S.A. (BIK S.A.) shows that in the first half of 2018, lending companies cooperating with BIK S.A. gained 77.4 thousand new customers. This is nearly 22.1% more than in the previous six months[205]. Figure 11 below shows a steadily increasing share of borrowers who do not have any loan liabilities towards banks. According to BIK S.A., more than half of them are young people, under the aged of 35.

Figure No. 11 - Customers of loan companies (in thousands), including persons servicing simultaneously bank loans according to BIK S.A[206]



514. The vast majority of loans offered by the so-called loan companies are loans of a relatively small amount, below PLN 50 thousand, which is indicated by data of BIK S.A. as well as by the results of the analysis conducted by the employees of the Banking Institute of the Warsaw School of Economics, presented below.

Table No. 21 - Structure of the non-banking loan market (2016)[207]

LOANS SECURED BY REAL ESTATE	LOANS REPAYABLE IN INSTALMENTS	MICRO-LOANS	
for 24-60 months with an average amount of PLN 20,000	*for 12-30 months with an average amount of PLN 5,000*	*for 14-90 days with an average amount of PLN 1,200*	
3%	22%	75%	*quantitatively*

[205] Loan Trends - Report for the 1st half of 2018. Semi-Annual Report of the Credit Information Bureau, p. 6 (available at: https://media.bik.pl/publikacje/read/406157/kredyt-trendy-raport-1-pol-2018-r).
[206] Ibidem, p. 6.
[207] Andrzej Bień, Łukasz Gębski, Report on credit risk and methods of its protection applied by non-banking financial institutions operating on the Polish market, Warsaw 2017, p. 12 (available at: http://www.instytutanalizrynkowych.pl/wp-content/uploads/2017/05/RYNEK-POŻYCZKOWY-W-POLSCE-RAPORT-NA-TEMAT-RYZYKA-KREDYTOWEGO-I-MOTOD-ZABEZPIECZANIA.pdf).

14%	63%	23%	*amount*

515. In accordance with information presented in Figure no. 7 (entitled: *Completed analytical proceedings instituted by GIFI in 2016-2018, broken down by products and services used for execution of suspicious transactions*, some analytical proceedings conducted by the GIFI concerned suspicious loans (understood as loans granted by entities other than banks, both professionally and privately) and donations.

516. The possibility to use these legal instruments for money laundering seems relatively simple: "A natural or legal person who derives profits from illegal activities and wishes to legalise them shall communicate with other persons with a view to drawing up a fictitious loan or donation agreement"[208]. However, loans - as opposed to donations - offer some additional opportunities to carry out transactions aimed at laundering property values derived from illegal activities. This is mainly due to the fact that the loan may involve various financial transactions (granting of a loan, repayment of principal and interest payments or payment of additional fees required by the lender).

517. The following elements that foster the use of loans for money laundering may be listed, following the replies to the surveys referred to in subchapter 5.3.1, as justification for indicating that a product or service is susceptible to money laundering:

- no obligation to register the borrowing of large amounts or a significant amount by one person (natural or legal);
- the difficulty in verifying the statements made by lenders and borrowers regarding their lending;
- possibility of transferring practically any amount of money without complicated formalities or documents;
- possibility of executing transactions in cash.

Life insurance

518. Insurance undertakings usually offer products whose characteristics do not permit rapid introduction and disbursement of funds. Their aim is to provide financial resources in the event of life-threatening or health-endangering situations. They are usually linked to a predefined amount of premiums paid by customers and a forecast payment in the event of an insurance event. The exception to the above rule are only insurance products linked with investment services.

519. According to the information of the Polish Chamber of Insurance, in 2017 the value of life insurance premiums amounted to PLN 24.6 billion (i.e. over 2.9% more than in 2016), including PLN 11.3 billion related to unit-linked insurance - UFK (i.e. over 45.9% of the value of all premiums)[209] At the same time, in the indicated period PLN 20.3 billion was paid out as claims and benefits under life insurance (i.e. over 10.9% more than in 2016).

[208] Counteracting money laundering and terrorist financing. A Guide for obligated institutions and cooperating units, Ministry of Finance, 3rd edition, Warsaw 2009, p. 74.

[209] Insurance in figures 2017. The insurance market in Poland in 2018, p. (available at: https://piu.org.pl/wp-content/uploads/2018/04/ubezpieczenia-w-liczbach-2017.pdf).

520. Although insurance products are relatively rarely used for money laundering, it should be noted that some risk exists in this area. The GIFI referred to it, pointing to their possible use for money laundering in the aforementioned guide for obligated institutions and cooperating units "Counteracting money laundering and financing of terrorism" of 200.)

521. Insurance products linked to investment elements are significant in terms of prevention of money laundering and financing of terrorism. *The Act of 11 September 2015 on insurance and reinsurance activity* distinguishes unit-linked life insurance as well as life insurance in which the benefit of an insurance company is determined on the basis of specified indices or other underlying values (class I, group 3 in the Annex to the aforementioned Act). These types of insurance whose purpose is not only the financial protection in case of random events but also investing free funds of the insured have been granted in Poland for many years. UFK, in which an insurance company invests its funds, is an integral part of the majority of them. According to the KNF (PFSA), "insurance companies offer many UFKs, differing in the structure of their investment portfolio, which has a direct impact on the level of investment risk of a given UFK"[210] Monetary resources originating from insurance premiums are partly transferred to a separate fund, i.e. UFK (managed by an insurance company or other specialised entity, e.g. an investment fund management company). Within this fund they are invested in shares, bonds, derivatives and other financial instruments according to the option chosen by the client.

522. "The value of a unit-linked insurance fund is converted, analogically to investment funds, into units. The division of the premium into parts serving the purpose of cover and investment depends on the value of the sum insured and the scope of risk of occurrence of random event effects covered by the insurance. For example, a higher sum insured or a large number of risks covered will result in spending a smaller proportion of the total premium paid by the customer on investments. Analogically, conversely low level of insurance cover makes it possible to construct a product that has primarily an investment value".[211] This way of construction of insurance products can encourage their use for money laundering.

523. In its "Guidance for risk-based approach - the Life Insurance Sector", the FATF presented examples of risks (*inherent risks*) associated with life insurance business. This document presents, among others, the following risks[212] of significance for the insurance market in Poland:

1) In the scope of products and services,

   - products related to high-risk payments (e.g. cash transactions, transactions consisting of multiple operations, transactions from third parties, cross-border transactions, potential withdrawals not related to a specific random event);

[210] UKNF (PFSA) position concerning the application of Article 21 of the Act of 11 September 2015 on insurance and reinsurance activity, KNF (PFSA), 23 October 2018, p. 2 (available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_w_sprawie_stosowania_art_21_ustawy_o_dzialalnosci_ubezpieczeniowej_i_reasekuracyjnej_63502.pdf).
[211] Letter from the Deputy Chairman of the KNF (PFSA) to the Chairman of the Senate Commission on Human Rights, Rule of Law and Petitions, no. D1U/070/2/2/2/2017, dated 17 October 2017, p. 3 (available at: https://www.senat.gov.pl/gfx/senat/userfiles/_public/k9/komisje/2018/kpcpp/materialy/197/002/9.pdf).
[212] Guidance for risk-based approach - the Life Insurance Sector, FATF, October 2018, pp. 21-22, available at: http://www.fatf-gafi.org/documents/riskbasedapproach/documents/rba-life-insurance.html?hf=10=0=desc(fatf_releasedate).

- products that accumulate high-value funds or enable execution of high-value transactions;
- products supporting anonymity or enabling easy transfer / disposal (e.g. bearer or secondary market policies);
- products enabling redemption before their maturity;
- uncomplicated products with low value gains.

2) In the scope of distribution channels,
   - sales channels without physical contact with the customer;
   - reliance on others and outsourcing (e.g. where an entity selling products and services on behalf of an insurance company is not well known to that company);
   - the management by insurance intermediaries of customer payments on their behalf and for their account (including execution of cash transactions or acceptance of payments for the account of an intermediary).

524. The risks listed above are largely compatible with those listed in the guidelines published in 2017 by the Joint Committee of the European Supervisory Authorities (i.e. *European Banking Authority* (EBA), *European Insurance and Occupational Pensions Authority* (EIOPA) and *European Securities and Markets Authority* (ESMA))[213]

5.3.2. Risk areas on the non-financial market

525. The questionnaires, which the GIFI distributed in 2017 to obligated institutions and cooperating units[214] included a request to indicate 5 products and services offered on the financial market which are or may be most frequently used for money laundering. Replies were selected from the list containing the following items:

- telecommunications services in the scope of increased payment numbers (Premium services);
- cryptocurrencies (e.g. Bitcoin, Monero);
- centralised convertible currencies used for the transfer of assets (e.g. Webmoney, Perfectmoney);
- physical transport of property values across the border by natural persons;
- cargo services, courier and postal parcels;
- purchase/sale of tokens in a casino;
- games on gaming machines;
- other games of chance;

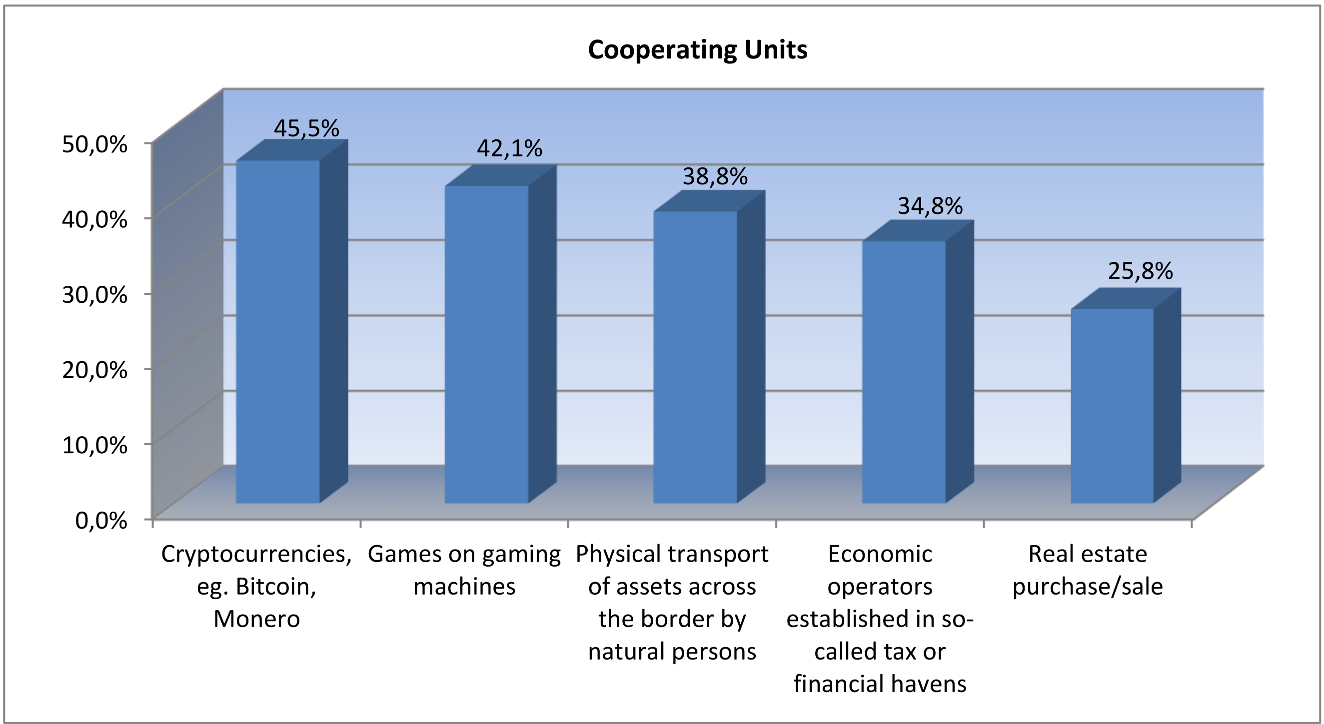
[213] Final Guidelines. Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions. The Risk Factors Guidelines, European Supervisory Authorities, June 2017, pp. 66-67 (see: https://eba.europa.eu/-/esas-publish-aml-cft-guidelines).

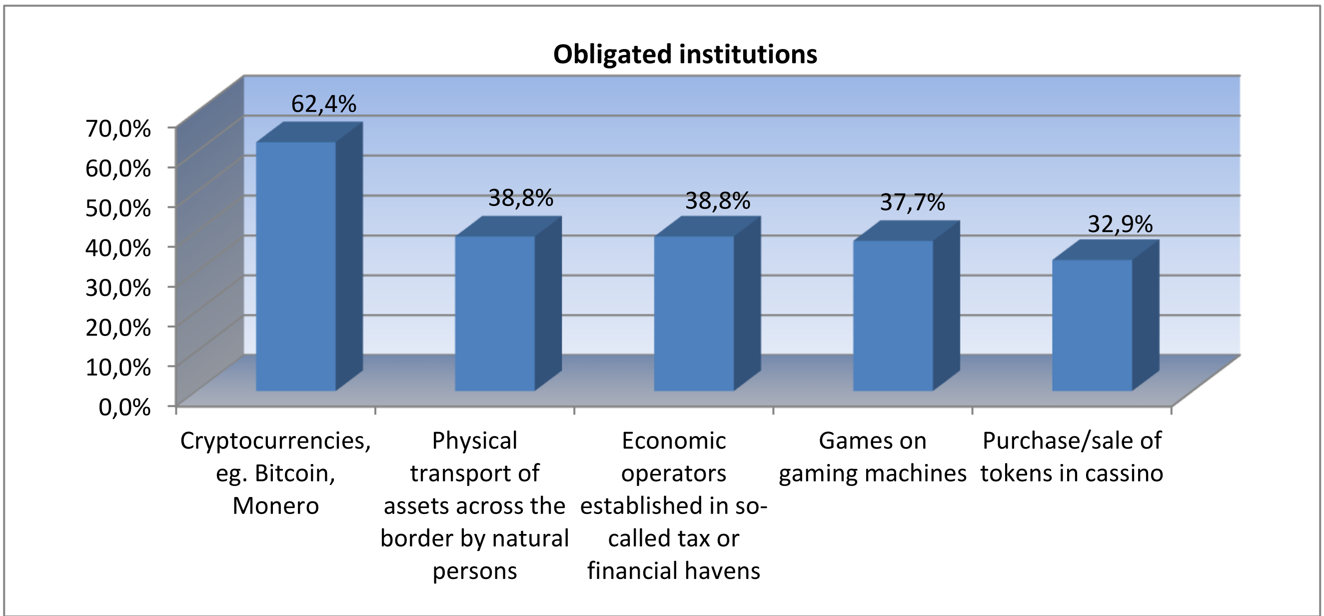
[214] For more information on them, see chapter 5.3.1.

- poker and other similar games;
- betting;
- online gambling;
- community financing ("crowdfunding" type);
- services of lawyers and legal counsels;
- services provided by notaries;
- services provided by statutory auditors and tax advisers;
- bookkeeping services;
- activities of non-profit entities (foundations, associations);
- purchase/sale of precious stones and metals;
- trade in antiques and works of art;
- trade in other high-value goods, e.g. cars, boats;
- purchase/sale of real estate;
- donation agreements;
- import/export of goods and services;
- business entities based in so-called tax or financial havens;
- trusts;
- companies that do not conduct economic activity in practice (simulation companies);
- services related to the creation and servicing of business entities and trusts;
- other products and non-financial services.

526. The list of 5 products and services indicated by the largest number of obligated institutions is identical to the list of 5 products and services indicated by the largest number of cooperating entities. The products and services indicated by both groups of entities in items 1 to 4 are the same (although in a different order). However, the products and services indicated in item 5 are different. The obligated institutions indicated the purchase/sale of tokens in the casino, while the cooperating units indicated the purchase/sale of real estate.

Figure No. 12 - Responses concerning products and services offered outside the financial market most frequently used for money laundering





527. Summing up, both cooperating units and obligated institutions which submitted their answers to the questionnaire survey questions indicated that cryptocurrencies, products and services related to gambling games, physical transport of property across borders and purchase/sale of real estate, are most frequently used for money laundering The risks associated with these areas (excluding cryptocurrencies described in chapter 5.3.1) as well as with other areas outside the financial market specified in the 2017 Report of the European Commission on

the transnational assessment of the risks of money laundering and financing of terrorism in the EU, are described below[215].

Cash circulation

528. According to the surveys conducted by the NBP in 2016 (questionnaire surveys and seven-day diary surveys), cash was a commonly used means of payment. In more than half of the cases (around 53.92% of transactions), consumers chose cash to make payments. However, the total value of these transactions (approx. 40.66% of the value of all payment transactions) was lower than the value of transactions executed by means of payment cards. Cash was therefore the most popular in terms of low-volume transactions (about 80% of transactions worth less than PLN 10)[216]

529. Cash, due to the anonymity of its users, is traditionally one of the favourite types of property values acquired by criminals in the framework of predicate offences[217] committed by them. Transactions in cash are also often used for money laundering, especially during the depositing phase when benefits from illegal sources are introduced into the financial system. The practice of the GIFI, however, shows that such transactions have been and are carried out at the subsequent stages of money laundering.

530. The Communication from the European Commission summarising the surveys ordered by it performed by ECORYS B.V. and the Centre for European Policy Studies to assess the potential impact of restrictions on cash payments on illegal activities and the internal market[218] indicates, among others, that "...cash transactions play an important role in money laundering, the main reason being that the proceeds of crime tend to take the form of large amounts of cash, although non-cash payments and new forms of crime are becoming increasingly important [...]. Cash is therefore often the starting point for money laundering and therefore requires certain cash transactions, often through the purchase of high-value goods".[219]

531. In the 2017 Report of the European Commission on the transnational assessment of the risks of money laundering and financing of terrorism in the EU[220], the European Commission devoted a great deal of attention to, inter alia, analysing the risk of money laundering and financing of terrorism in relation to so-called *cash products*. It pointed to the use of couriers to transport cash related to illegal activities, in particular high denomination banknotes (underlining that the higher the value of the banknotes transported, the more cash can be

---

215 Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 June 2017, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

216 Arkadiusz Manikowski, Reasons for frequent cash selection by Poles - analysis of the results of the 2016 survey and diary survey, NBP 2017, p. 3-4, available at: https://www.nbp.pl/badania/seminaria/13xii2017.pdf.

217 During officially conducted activities in connection with the detention of persons suspected of committing an offence, law enforcement officers often detect significant amounts of cash held by the perpetrators - see: http://cbsp.policja.pl/cbs/aktualnosci/149197,Narkotyki-w-magazynach-majatek-przepisany-na-3-letnie-dziecko-CBSP-i-Prokuratura.html, https://www.strazgraniczna.pl/pl/aktualnosci/7243,Zabezpieczono-prawie-dwa-miliony-zl-z-przestepczej-dzialalnosci.html

218 Conducted in 2017 and completed in February 2018.

219 Report from the Commission to the European Parliament and the Council on restrictions on cash payments, Brussels, 12 June 2018, p. 8, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557325306958ri=CELEX:52018DC0483.

220 Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Brussels, 26 June 2017, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

transported in a limited space) as well as *cash intensive business* and cash payments. The risk levels associated with these products have been determined by the European Commission as high or very high.

532. The Europol publication of 2015 addressed the issue of the relatively high share of high denomination banknotes in euro in cash circulation between 2002 and 2014. It was noted that EUR 500, EUR 200 and EUR 100 banknotes accounted for approximately 54% of all banknotes in circulation and that the value of all 500 EUR banknotes amounted to approximately 54% of all banknotes in circulation[221]. This was strange since the surveys earlier conducted by the European Central Bank (ECB) reported that around 56% of respondents had never encountered a EUR 500 banknote and around 44% of respondents had never held a EUR 200 banknote.[222] Additionally, Europol stressed that in many cases companies did not accept payments with such high denomination banknotes for purely practical security reasons (e.g. fraud risk). Furthermore, it stated that, based on indications from international anti-money laundering proceedings, 500 EUR denomination banknotes were the favourite tool used by criminals to accumulate profits from illegal activities outside the financial system.[223]

533. In connection with the foregoing, the European Commission welcomed the ECB's decision of 4 May 2016 on cessation of issuing 500 EUR[224] banknotes, indicating that this should contribute to reducing the risk of money laundering associated with cash payments[225]

534. In Poland, relatively small denomination banknotes remain in circulation[226] (the highest denomination - PLN 500, was introduced to circulation by the NBP in February 2017). The number of banknotes with the highest denominations in circulation is relatively small, with more than 7.2 million banknotes in circulation at the end of 2017 Q4, representing only 0.4% of the total number of banknotes in circulation[227]. The share of the PLN 500 denomination in the value structure of banknotes remained relatively low at the end of 2017 Q4 and amounted to approx. 1.9%. On this basis, it cannot therefore be concluded that, as in the case of high denomination euro banknotes, they can often be used for money laundering purposes.

535. Cash related to profits from illegal activities is also physically transported by so-called cash couriers or using postal service or a specialised courier service. For example, in the framework of the "Kouri" operation in 2016, a Joint Investigation Team (JIT) composed of

[221] Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering, EUROPOL Financial Intelligence Group, 2015, s.14, available at: https://www.europol.europa.eu/sites/default/files/documents/europolcik (1).pdf.
[222] The use of euro banknotes - results of two surveys among households and firms, w: Monthly Bulletin - April 2011, ECB, p. 85, available at: https://www.ecb.europa.eu/pub/pdf/other/art2_mb201104en_pp79-90en.pdf.
[223] Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering, EUROPOL Financial Intelligence Group, 2015, p.14, available at: https://www.europol.europa.eu/sites/default/files/documents/europolcik (1).pdf.
[224] Most euro area national central banks issued them until January 2019, while the Deutsche Bundesbank and Österreichische Nationalbank issued them until April 2019. (https://www.bundesbank.de/de/aufgaben/themen/herstellung-und-ausgabe-des-500-euro-scheins-wird-eingestellt-599234date of reading 2 May 2019)
[225] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 26 June 2017, p. 13, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.
[226] In particular, if their value to that of euro banknotes is compared.
[227]Report on the Cash Circulation in Poland in 2017, NBP, December 2018, p.11, available at: https://www.nbp.pl/home.aspx?f=/publikacje/gotowkowy/gotowkowy.html.

French, Belgian and Dutch investigators and representatives of Eurojust and Europol, revealed a group dealing with laundering money originating from drug trafficking. Cash couriers collected up to EUR 1 million in cash each month travelling across Western European countries and then transported the money to Belgium and the Netherlands, from where it was transferred via the *Hawala* system to Morocco via the Middle East. More than EUR 7,1 million in cash was secured in the framework of the operation[228]

536. Another operation, carried out by the CBŚP in May 2019 together with the Lithuanian, UK, Estonian and Spanish law enforcement authorities in the framework of the Joint Operational Task Force established in Europol in November 2018, was the operation code-named "Icebreaker". Its aim was to break up an international criminal group involved in drug trafficking and the marketing of large quantities of psychotropic substances, cigarette offences and laundering money originating from this process. It consisted mainly of Lithuanian citizens, however, Poles also dealt with money laundering.[229]

537. In accordance with the investigators' findings, as early as 2015, relatively high amounts of money from the illegal activities of the aforementioned group (mainly cigarette crimes and drug smuggling, mostly hashish from Morocco and cocaine from Colombia) were transported from Great Britain to Poland, from where, inter alia, via the Netherlands they were transported to other countries, including Colombia. Cash was transported by various methods, including air transport and also by lorries (even up to GBP 50 million could be smuggled in truck transport in a single operation). In Poland, the money was transferred to bureaux de change offices cooperating with the criminal group.

538. According to published information, in 2016, members of the aforementioned criminal group smuggled more than 2 tonnes of cocaine from Colombia to Romania in 2016, to be subsequently transported to the Netherlands, and introduced more than 150 kg of cocaine into the market in the United Kingdom. As early as in 2017, the CBŚP thwarted the smuggling of over 200 kg of hashish from Spain to Poland by members of this group.

539. It is estimated that only in the years 2017-2019 the above-mentioned criminal group was able to obtain profits of nearly EUR 680 million from the activity pursued.

540. On 15-16 May 2019, the total of more than 450 officers of the Polish, British, Spanish, Lithuanian and Spanish services, supported by Europol and Eurojust, carried out a coordinated action under the "Icebreaker" operation. In Poland, Lithuania, Great Britain and Spain the total of about 40 searches and detentions of 22 persons were carried out, including a Lithuanian citizen suspected of managing the criminal procedure. Almost EUR 8 million was also seized, mainly in cash, gold bars, jewellery and diamonds (as well as certain quantity of illegal cigarettes).

541. In the framework of this operation, Polish officers operating in the Pomorskie, Dolnośląskie and Opolskie Provinces detained 8 suspects (the ninth person was arrested on 17

---

[228] European Union serious and organised crime threat assessment. Crime in the age of technology, Europol, 2017, p. 18 (available at: https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment).

[229] http://policja.pl/pol/aktualnosci/173762,Podejrzani-mogli-wyprac-680-mln-euro-operacja-Lodolamacz.html, date of reading 23 May 2019 and https://www.europol.europa.eu/newsroom/news/operational-task-force-leads-to-dismantling-of-one-of-europe's-most-prolific-crime-groups-behind-€680-million-operationreading date 23 May 2019

May 2019). In addition, cash in various currencies (including EUR, GBP, USD, PLN, NOK, SEK) as well as a money counting device and other property belonging to suspects, including vehicles, collector coins and jewellery, were seized, with the value equivalent to approximately PLN 10 million.

542. In accordance with Article 85(1) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the GIFI receives information from the Border Guard authorities and the KAS from the declaration of cash transport across the EU border.

543. In 2018, it received 11,116 notifications concerning declarations of imports of funds into the EU and 771 notifications on declarations of exports of funds from the EU. Moreover, the GIFI also received information concerning 701 notifications from the declarations of the transport of funds between EU countries and 366 declarations of the transport of funds between non-EU countries. The number of notifications arising from declarations submitted by the Border Guard bodies and the KAS bodies in 2018 increased by approximately 10% in relation to 2017. Accordingly, the total value of amounts reported in the declarations of funds imported into the EU increased (by about 6.3%, to PLN 1,231 million). On the other hand, the summarised amount in PLN for funds declared as exported from the EU decreased in comparison to 2017 by approx. 12.3% and amounted to PLN 136.4 million in 2018.[230]

544. In terms of total value, most cash was declared as imported into the EU in 3 currencies, i.e.:

- EUR 156.6 million;
- USD 95.5 million;
- PLN 149.6 million.

545. Cash exports to the EU were declared in the same currencies:

- PLN 66.6 million;
- USD 9.6 million;
- EUR 5.4 million.

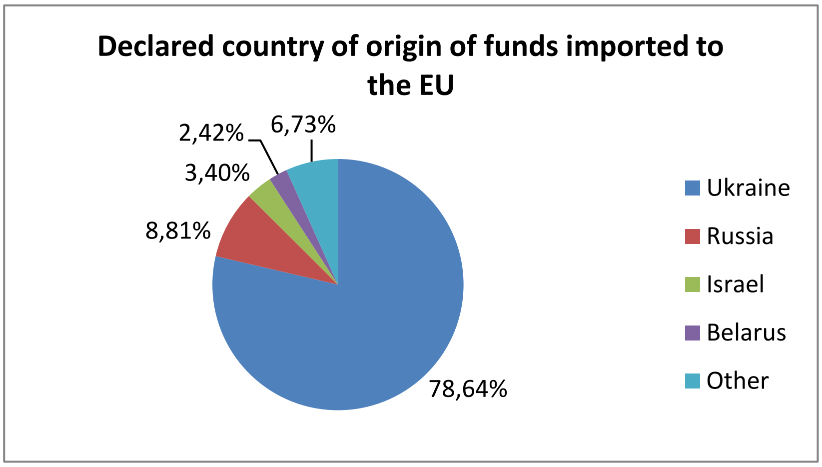
546. Imports were most frequently declared (as in 2017) by citizens of Ukraine (in approx. 76.40% of cases), followed by citizens of Russia (in approx. 7.29% of cases), Poland (in approx. 4.47% of cases), Israel (in approx. 3.56% of cases) and Belarus (in approx. 2.16% of cases), and in addition, by citizens of 65 other countries. On the other hand, exports were most often declared by citizens of Israel (in about 32.56% of cases - in 2017 they occupied the third position), Poland (in about 28.92% of cases), Russia (in about 9.60% of cases), Ukraine (in about 4.28% of cases), the Philippines (about 4.02% of cases) and, moreover, citizens of 35 other countries[231]

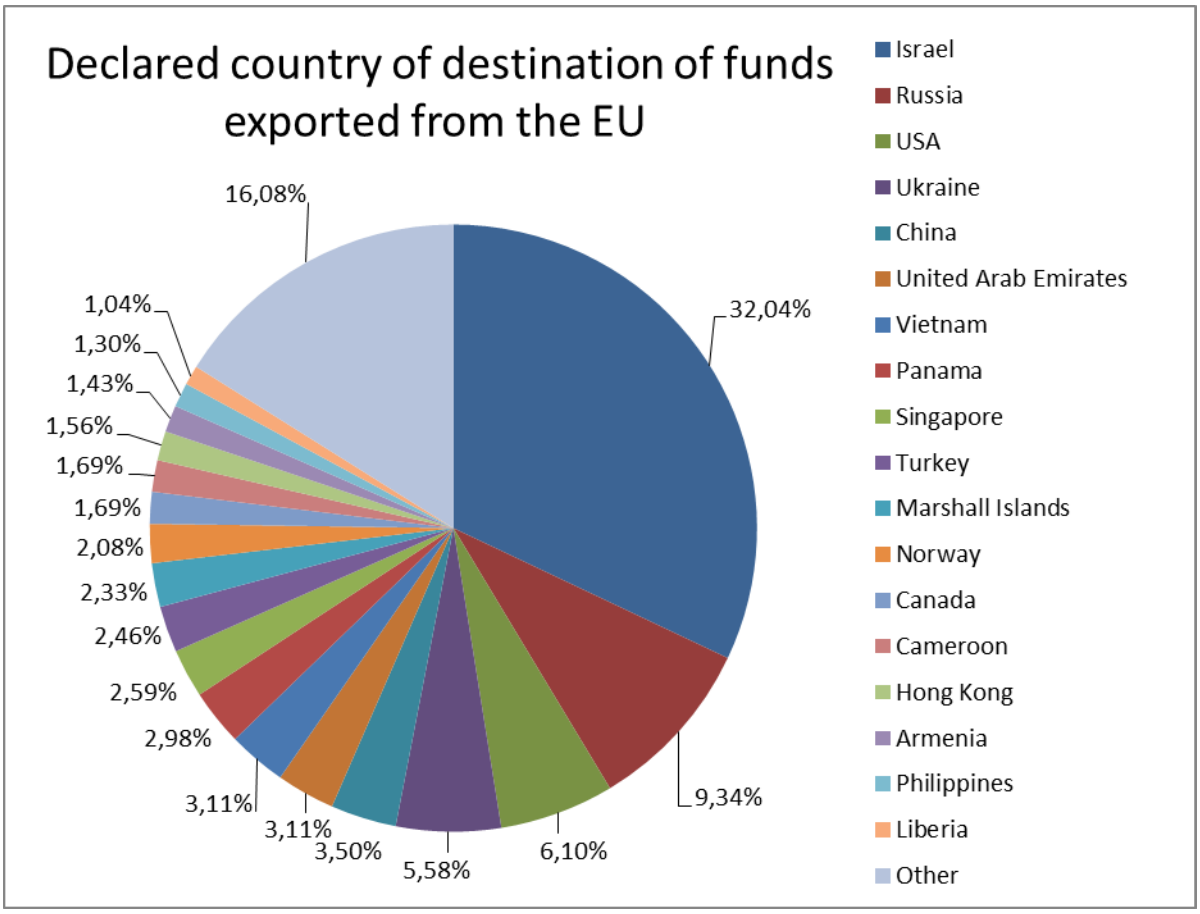
547. In terms of directions from which the funds were imported into the EU, as much as 78.64% of declarations regarded funds imported from Ukraine, 8.81% from Russia, approx. 3.40% from Israel; moreover, exports from 58 other jurisdictions were declared. In case of exports of funds

[230] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, Warsaw 2019, pp. 32-33.
[231] Ibidem pp. 34-35.

from the EU, declarations were most often related to their transport to Israel - about 32.04% of cases, Russia - about 9.34%, the USA - about 6.10%, Ukraine - about 5.58% (in other cases, exports to 52 other jurisdictions were declared).

Figure No. 13 – Imports/exports of funds according to the destinations declared in 2018[232]





548. As part of their official activities, the Border Guard and the KAS bodies sometimes detect cash transport without declaring it in accordance with the provisions of *Regulation (EC) No*

[232]Ibidem, p. 35.

1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community (OJ L 309, 25.11.2005, p. 9) and the *Act of 27 July 2002 - Foreign exchange law*. Information on such arrangements is also provided to the GIFI as part of the performance of the obligation referred to in Article 83 of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. They often relate to the transport of undeclared cash by nationals of other countries, in particular non-EU nationals, coming from the East. In some cases, such persons were linked to payment accounts held with Polish financial institutions, to which cash deposits were made and the funds deposited were transferred further abroad. There were also cases of informing the GIFI about undeclared transport of considerable amounts of money by Polish citizens detained in other Member States. They referred, for example, to persons who did not declare any income and simultaneously carried out financial transactions of significant value as well as persons who smuggled various goods at the same time, such as items used for the illicit manufacture of nicotine products.

549. In its report on the transnational assessment of the risk of money laundering and financing of terrorism, the European Commission drew attention, among other things, to the threat of using economic activities associated with large cash turnover for money laundering. These include, for example, catering companies, construction companies, retailers of various goods, pawnshops, antique shops, commission shops and gambling operators. In particular, they may be used to mix revenue derived from illegal activities with revenue derived from legitimate business activities. Frequently, these are also companies which only apparently conduct business activities and are used exclusively for money laundering and committing other crimes (so-called simulation companies)[233]

550. In addition, the European Commission has highlighted the possibility for criminals to use cash transactions to sell goods originating from illegal activities for cash, make various other payments, e.g. related to transport costs. While they certainly see problems with the introduction and continued use of such cash in the legal financial transactions, they still desire its use.[234]

551. A relatively high value of cash transactions may be conducive to concealing the use of cash for money laundering. In the recent years, i.e. between 2010 and 2017, the share of cash in the M1 money supply aggregate in Poland stabilised in the range between 20% and 22% (in 2017 it amounted to 20.4% and was higher by 5.4 percentage points than the EU average and by 6 percentage points than the euro zone average)[235]. At the same time, however, the share of cash in Poland's GDP in 2017 amounted to 9.5% and was lower than the average for the euro area by 0.5 percentage point, although it was 0.4 percentage point higher than the EU average. In this area, Poland - against the background of the situation in other EU countries - has quite a positive image. It is in the middle of the stakes, ahead of Bulgaria, Hungary and the Czech

---

[233] This concept is explained in Chapter 5.4. in the context of the money laundering methods used.

[234] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 30-31 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[235] Comparison of selected elements of the Polish payment system with systems of other EU Member States for 2017, NBP, December 2018, pp. 40-41, available at: https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2017.pdf.

Republic (with Romania, Croatia, the United Kingdom, Denmark and Sweden reporting lower rates)[236]

Crowdfunding

552. In the 2017 Report on the transnational assessment of the risks of money laundering and financing of terrorism in the EU, the European Commission has devoted a great deal of attention to the risk analysis of so-called *crowdfunding*, which is carried out via platforms made available on the Internet. Among others, it indicated the possibility of collecting funds for fictitious purposes and transferring them abroad for the purpose of money laundering or financing of terrorism.[237] At the same time, it encouraged EU Member States to consider including crowdfunding in anti-money laundering and counter-financing of terrorism legislation[238]

553. There are many definitions of crowdfunding of various level of details, however, they contain common elements through which it is possible to determine what is meant by this term:

- the financial support of funders is always of financial nature,
- the collection is carried out via the Internet,
- the funders receive various kinds of awards for their contributions (the so-called "refundable benefit"),
- the fundraising action is usually undertaken within a specified time interval,
- the financing campaign is open on two levels, i.e. anyone can make a donation from anywhere and in any amount; it is clear who collects the money, for what purpose and what amount of money is to be raised.[239]

554. However, it should be noted that funders do not always receive refundable benefits for their contributions, e.g. in the case of so-called grant *crowdfunding* .

555. Crowdfunding can take various forms, e.g.:

- Grant *crowdfunding* - collecting money for a specified purpose without the execution of the mutual benefit of the project provider / beneficiary;
- Award-based *crowdfunding* - in exchange for the contribution of funds, the funders receive a specific kind of gratification which does not necessarily have to be the economic equivalent of the funds contributed;

[236] Ibidem, p. 42.
[237] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 52-56 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.
[238] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 26 June 2017, p. 18, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.
[239] Justyna Małgorzata Ziobrowska, Crowdfunding as a modern form of supporting social, cultural and business ventures, in: Finance, Financial Markets, Insurance No. 3/2016 (81), p. 287, available at: http://www.wneiz.pl/nauka_wneiz/frfu/81-2016/FRFU-81-285.pdf.

- Pre-sale based *crowdfunding* - the funders provide money to create a product that is delivered to them by the beneficiary after a certain period of time;
- Share-based *crowdfunding* - the funders invest in the beneficiary's undertaking, receiving share units in the share capital of its company;
- Debt *crowdfunding* - the funders' benefit provided to the beneficiary is refundable, i.e. the beneficiary undertakes to return the money received.[240]

556. According to the European Commission report on crowdfinancing in the EU, the following types can be also distinguished:

- *invoice trading crowdfunding* - the beneficiary transfers unpaid invoices or receivables (single or in a package) to the funders in exchange for cash;
- *hybrid models of crowdfunding* - a model containing an element of various types of *crowdfunding.*[241]

557. In accordance with the survey conducted in 2018 by the Startup Poland Foundation, among startups, 11% of the respondents indicated the intention to raise capital through crowdfunding. At the same time, startups' hopes associated with participation in share-based *crowdfunding* are increasing[242]

558. Crowdfunding enables raising the necessary capital in a fast and easy way, without fulfilling obligations related to e.g. obtaining a loan or borrowing from credit and financial institutions, offering shares of a company in a traditional public offering or a time-consuming search for financing among *venture capital* funds . According to the Polish Agency for Enterprise Development (PARP), this method of financing is used mainly by small and medium-sized enterprises. It is particularly popular among "relatively young and modern companies dealing with new technologies or other projects whose assumptions are easy to present in electronic media".[243]

559. Although it is possible that *crowdfunding* is limited to a bilateral relationship between the funder and the beneficiary, *crowdfunding* platforms often act as intermediaries between them. On the Internet there are numerous cases of such platforms, also offering services in Polish. For example, one of them advertises its services indicating that "it helps young businessmen to raise capital [...] entrepreneurs can raise capital to start business from the community of Internet users. We set one condition - the entrepreneur looking for financing must offer the supporters shares in the undertaking in exchange for the support."[244] Another platform, on the other hand, indicates the possibility of carrying out through it a fund-raising campaign not only of a public but also of a private nature (a request for financing is addressed by the beneficiary only to

[240] Jacek Czarnecki, Types of crowdfunding, in: Crowdfunding, collective work, Wardyński i Wspónicy, Warsaw, September 2014, pp. 8-9, available at: https://newtech.law/wp-content/uploads/2017/08/raport-o-crowdfundingu.pdf

[241] Commission staff working document. Crowdfunding in the EU Capital Markets Union, European Commission, Brussels, 3 May 2016, pp. 8-9, available at: https://ec.europa.eu/info/system/files/crowdfunding-report-03052016_en.pdf.

[242] Polish startups. Report, 2018, ed. Startup Poland Foundation, Warsaw 2018, p. 36, available at: http://startuppoland.org/knowledge/.

[243] https://www.parp.gov.pl/component/content/article/54127:crowdfunding-zasady-dzialania-i-europejskie-plany-regulacyjne , date of reading 02 May 2019

[244] http://startuppoland.org/startup/crowdfunding/ , date of reading 2 May 2019

specific recipients, e.g. acquaintances)[245]. According to its information, 300,603 fund-raising campaigns (collecting money) were conducted through it until 7 May 2019[246] but only about 3.6% of them were public. Within their framework, the beneficiaries collected over PLN 99.93 million, transferred through over 1,556,783 transactions (which gives an average transaction value of about PLN 64.19). Since 2 May 2019, the number of campaigns has increased by 2,305, including 63 public campaigns. Within 5 days, owing to this platform, over PLN 0.93 million was raised within approx. 14.5 thousand transactions[247]

560. The information contained on the website of another *crowdfunding* platform specialising in share-based *crowdfunding* shows that by 8 May 2019[248], 48 issues during which over PLN 24.35 million from 22,118 investors were raised[249] have been performed through the platform.

561. Some *crowdfunding* platforms additionally offer other services, such as developing clients' ideas with the use of knowledge, experience and creativity of a wide community or establishing a joint stock company, marketing, legal and other services (e.g. preparation of share sales documents, the prospectus, legal services after a successful issue or handling share dispatch).

562. Crowdfunding is an innovative economic phenomenon, which also affects its understanding from the legal point of view. There are no comprehensive provisions regulating this phenomenon. From a civil law point of view, entities participating in crowdfunding use the freedom of contract. Legal relations concluded in its sphere are usually based on the most popular types of agreements, adapted to specific models of crowdfunding (e.g. agreements on donations, loans, sales, etc.)[250]

563. The threat of using crowdfunding for money laundering is based primarily on its attributes, such as:

- lack of legal provisions relating explicitly to the above-mentioned phenomenon, including regulating the rules of arranging crowdfunding campaigns and identifying and verifying clients of *crowdfunding* platforms;
- lack of supervision over the functioning of *crowdfunding* platforms;
- far-reaching anonymity of persons and entities financing the beneficiary;
- possibility of implementing investments of international character.

564. Currently, *crowdfunding* platforms are not obligated institutions under the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, unless they are subject to the provisions of the aforementioned normative act in connection with their provision of additional services (e.g. payment services, currency exchange or services referred to in Article 2(1)(16) of the aforementioned Act). Therefore, they are not obliged to apply customer due diligence measures or to transfer the information specified in the above mentioned Act ex officio and upon request to the GIFI.

[245] Private collections are unlikely to be classified as crowdfunding because of the closed circle of recipients.
[246] The company operating this platform was established in August 2016.
[247] Https://zrzutka.pl/,, dates of reading 2 May 2019 and 7 May 2019.
[248] The platform was launched in August 2012.
[249] https://beesfund.com/ , date of reading 8 May 2019
[250] Jacek Czarnecki, Krzysztof Wojdyło, Loan, donation or pre-sale? Legal constructions used in crowdfunding, in: Crowdfunding, collective work, Wardyński i Wspónicy, Warsaw, September 2014, pp. 14-16, available at: https://newtech.law/wp-content/uploads/2017/08/raport-o-crowdfundingu.pdf

565. In addition, *crowdfunding* platforms operate on the basis of the provisions of *the Act of 6 March 2018 - Entrepreneur law* and are not subject to supervision by specialized state authorities (with the exception of those whose activity falls within the scope of the regulations governing the functioning of the financial market).

566. While *crowdfunding* platforms usually identify project beneficiaries, they rarely do so in the case of funders. In addition, forms of financing are sometimes allowed which may additionally contribute to the concealment of funders' data (e.g. cryptocurrencies or prepaid phone cards[251] issued by some foreign operators without registration of their users, which are then resold by the beneficiary). Moreover, international transactions are possible through *crowdfunding* platforms, which may also make it difficult to identify funders who carry out transactions from other countries[252].

567. Therefore, the following main threats associated with the activity of *crowdfunding* platforms can be mainly indicated:

- opportunity of mixing profits from legal and illegal sources;
- possibility of anonymous transfer of property values originating from criminal activity to third parties;
- possibility of legitimising the property values originating from criminal activity by indicating their origin from *crowdfunding* actions;
- possibility of practical sales of property values originating from criminal activity by transferring them as refundable benefit for the funds received.

Telecommunication services linked with mobile payments

568. The European Central Bank applies a definition of mobile payments which[253] states that they are payments where payment data and payment orders are initiated, transmitted or confirmed using mobile devices and technologies enabling communication and data transmission between the payment service provider and the consumer. Mobile payments are often identified with Internet payments. The difference between these payments, however, lies in the way in which the transaction is performed. In the case of Internet payments, a website dedicated to payments or the bank's Internet banking website is most commonly used. On the other hand, in the case of mobile payments, however, we deal with a transaction that is most often performed using an application specially created for this purpose, installed on a mobile device.

[251] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, p. 54 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[252] "For the success of crowdfunding campaigns it is particularly important to reach as many interested potential investors as possible whereas their nationality or place of residence are usually of little importance. Therefore, crowdfunding campaigns of international and cross-border character are most successful - they are the ones able to collect the largest funds in the shortest possible time" – https://www.parp.gov.pl/component/content/article/54127:crowdfunding-zasady-dzialania-i-europejskie-plany-regulacyjne date of reading 2 May 2019

[253] https://bankionline.com.pl/platnosci-mobilne/ , date of reading 21 May 2019

569. In accordance with the definition contained in Wikipedia, mobile payments[254] (also referred to as "m-payments") are non-cash payments made via a mobile device, such as a smartphone, a tablet or a mobile technology, such as SMS, NFC, USSD, WAP. Mobile devices used for making payments must allow for connectivity to the telecommunications network (GSM or Internet). Mobile payments enable direct purchase of goods or services and the transfer of money between the bank accounts of the buyer and the seller. This definition divides payments according to the way the mobile device communicates with the data processing centre and distinguishes:

1) Remote mobile payments as the most popular type of m-payment. It is based on the connection between a mobile phone and a server via SMS (so-called Premium SMS) or the Internet. Premium SMS is most often used as a form of payment for press articles available on the Internet, participation in competitions, voting in television programs or online access to video materials. The Buyer enters the code indicated by the Seller in the SMS message and sends it to number provided. In response, he/she receives a return message confirming sending of the SMS or a code that can be entered on the website and thus unlocks access to the content searched for.

2) Proximity mobile payments, which currently occur in the NFC (*Near Field Communications*) technology. This wireless technology is based on the use of radio waves to exchange data over short distances, usually a few centimetres. Payment cards with the NFC technology approach the authorisation device, so that the connection is established and the data transfer takes place (a fee). It has been assumed that for transactions not exceeding PLN 50 there is no need to enter a PIN code. It improves and speeds up the payment process. The NFC technology also works in mobile phones, which thanks to it also become mobile wallets. They work in the same way as payment cards, i.e. a phone is placed close to the terminal in order to make a payment. An example of an application using the described technology is e.g. MyWallet. Owing to the fact that the phone is equipped with the aforementioned application, the user can make payments by bringing the phone closer to the payment terminal.

570. In the Report entitled "Digital Payments 2018"[255] prepared on behalf of the Chamber of Electronic Economy, which describes the subject of digital payments used by Poles, shows the relationship between *online*, mobile and *offline* payments. It turned out that answering to the question about their financial and transactional products, respondents indicated payment cards (40% of responses) and bank accounts with active Internet access (34%) as two most popular products in 2018. On the other hand, respondents indicated the BLIK Mobile Payment System, which is present in over a dozen Polish banks on the third place. With the result of 25%, it was indicated as the third most popular financial product that Poles hold.

571. Among mobile financial products, apart from BLIK, the survey respondents also included such products as Apple Pay, Google Pay payment[256] or payments by Garmin Pay watch and

[254] https://pl.wikipedia.org/wiki/P%C5%82atno%C5%9Bci_mobilne , date of reading 21 May 2019
[255] Digital payment report 2018, Chamber of Electronic Economy, available at: https://eizba.pl/wp-content/uploads/2018/12/Platnosci_Cyfrowe_2018.pdf.
[256] Google makes it possible to check on the website https://support.google.com/pay/answer/7352136 whether a particular Polish bank participates in the programme and whether the card will work with Google Pay (date of reading 21 May 2019).

Fitbit Pay[257]. Among them, *apple* payments and Google payments were indicated as most popular (based on declarations of 8% of users for each).

572. According information contained on the Juniper Research portal[258], one of the leading analytical companies in the *Fintech & Payments* sector, the most popular mobile payment method in the world today is Apple Pay. Almost 140 million users worldwide (out of a total of 241 million users of m-payment products) used this product in 2018, almost twice as many as all other m-payment products (such as Google Pay, Samsung Pay, etc.) combined. Analyses of Juniper Research shows that by 2020 the number of users of contactless mobile payments will exceed 760 million, compared to an estimated 440 million users in 2018. On the other hand, according to the same estimates, the number of users of mobile payment systems such as Apple Pay, Samsung Pay, Google Pay and others will reach 449 million worldwide by 2020. Apple Pay is estimated to be used by every second user of proximity mobile payments.

573. The aforementioned report of the Chamber of Electronic Economy "Digital Payments 2018" and the NBP report "Assessment of the functioning of the Polish payment system in the second half of 2018" show that BLIK is most popular in Poland among mobile payment products. The BLIK Mobile Payments System[259] was launched in February 2015 by Polski Standard Płatności sp. z o.o. (hereinafter referred to as the PSP), established by six commercial banks. The service of clearings with the BLIK system participants is provided by Krajowa Izba Rozliczeń S.A., which also provides the necessary ICT infrastructure. At the beginning it should be emphasised that within the BLIK Mobile Payments System, a payment system within the meaning of Article 1(1) of the *Act of 24 August 2001 on settlement finality in payment and securities settlement systems and rules of supervision over such systems, can be distinguished.* (Journal of Laws of 2019, item 212, as amended) as well as services provided under the payment scheme[260]. The P2P payment service is included in the second of the aforementioned categories.

574. The BLIK Mobile Payments System is included by the NBP among the main payment systems in Poland. In accordance with the NBP cyclical report "Assessment of the functioning of the Polish payment system in the second half of 2018", at the end of the second half of 2018, 8 main payment schemes operated in Poland[261]:

- 2 large-value payment systems: SORBNET2 system, operated by the NBP and TARGET2-NBP system, operated by the NBP in legal terms and by three central banks in operational terms (Deutsche Bundesbank, Banque de France and Banca d'Italia);

[257] See chapter 5.2.4 for a description of the way of operation and technical requirements of Apple Pay, Google Pay, Garmin Pay and Fitbit Pay. Innovative payment instruments in the NBP report - Assessment of the functioning of the Polish payment system in the second half of 2018, May 2019.

[258] https://www.juniperresearch.com/press/press-releases/apple-pay-accounts-for-1-in-2-oem-pay-users , date of reading 21 May 2019

[259] Spot payment systems - analysis of selected systems, role of the central bank and directions of development, NBP, June 2015, available at: https://www.nbp.pl/systemplatniczy/platnosci-natychmiastowe/systemy-platnosci-natychmiastowych.pdf.

[260] Article 2(26a) of the *Act of 19 August 2011 on payment services* defines a payment scheme as "a set of rules concerning processing of payment transactions, issuing and acceptance of payment instruments and processing of payment transactions performed with the use of payment instruments and the payment card scheme".

[261] Assessment of the functioning of the Polish payment system in the first half of 2018, NBP, May 2018, p. 18, available at: https://www.nbp.pl/systemplatniczy/ocena/ocena2018_2.pdf

- 6 retail payment systems: Elixir, Euro Elixir and Express Elixir systems - operated by Krajowa Izba Rozliczeniowa S.A., BlueCash system - operated by Blue Media S.A., BLIK system - operated by Polski Standard Płatności Sp. z o.o., KSR system - operated by First Data Polska S.A.

575. The BLIK system enables making payments with the use of mobile devices (e.g. mobile phones and tablets) both over the Internet and in traditional shops and service points, in public transport, public offices and between users (P2P). At the end of 2015, the Polish Payment Standard introduced the P2P service, i.e. mobile payments between mobile phone users, as part of the BLIK system. The service allows for immediate transfer of funds to the other person without the need to provide a bank account number, only by entering his or her phone number. In order to activate the service, the BLIK system user only has to link his or her phone number with the bank account number in the application. Transactions can be carried out with a portable device since 9 February 2015. The services can be used after downloading the mobile application of one of the BLIK system participants. At the end of 2018, the range of the BLIK system covered:

- 11 banks (the number of banks has not changed over half of the year);
- 8.8 million users (the number of registered BLIK mobile applications in the second half of 2018 increased by 2.2 million);
- 384 thousand retail and service outlets (over half of the year, 96 thousand new outlets were established);
- 413.8 thousand payment terminals (136 thousand new terminals were established over half of the year);
- 91.8 thousand online shops (over half of the year, 5.2 thousand new shops were opened);
- 19.8 thousand ATMs (2.1 thousand new ATMs were launched over half of the year).

576. In the second half of 2018, in total, 58 million orders were executed in the BLIK system (by approx. 77% more than in 2017) with the total value of PLN 7.8 billion (also by approx. 77.3% more than in 2017), on average, 315 thousand orders with the total value of PLN 42.1 million were executed daily and the average value of the order was PLN 134.[262] Following the increase in the total number of transactions processed by the system, a significant increase in the daily number of transactions was noted (the average daily number of settled orders in the second half of 2018 amounted to 315 thousand, compared to 181 thousand in the previous period).

577. Mobile payments are exposed to risks associated with various types of scams and frauds[263] Most of them involve phishing since approximately 71% of sellers identify such frauds. Consequently, perpetrators can take over a credit card, a mobile device (including a SIM card) or a loyalty program from which points can be used to make payments. Another fraud is so-called *pharming* (identified by 66% of sellers). It consists in redirecting the user to a fake website and taking over his/her password, account details or credit card details. The object of these activities are both the users of the shopping services and the suppliers themselves who are

[262]Ibidem, p. 47.
[263] https://fintek.pl/oszustwa-podazaja-rozwojem-platnosci-mobilnych/ , date of reading 21 May 2019

attacked by means of hacking software. More and more often, it takes the form of an exchange of fake information between the service and its unaware users. There is also so-called "friendly" extortion in which criminals inform the company that the card which was used for the transaction was stolen and ask for a refund.

578. In one of its reports, the FATF indicated which risk factors are associated with the use of mobile payments[264] It notes that mobile payment services can be used even without establishing a direct business relationship. The sole business relationships between a supplier and a user of mobile payment services can be established through agents, *online* or through the mobile payment system itself. Such mobile payment services exposed to the risk of anonymity may enable anonymous products existing in the market, particularly in other jurisdictions, to be made available - in particular prepaid cards - which can be connected to m-payment services. Verification of the customer's identity may be difficult in such a case. While the mechanisms for monitoring and reporting suspicious transactions themselves can work effectively, the lack of effective identification of a m-payment user can create problems. However, the specific financial institutions decide whether their cards will work with mobile payment products such as Google Pay or Apple Pay. A particular financial institution may limit the possibility to make mobile payments in the case of some or all cards.

579. Mobile payment services can be used to transfer funds virtually anywhere in the world or can be used in certain geographical areas. However, on 3 December 2018, the provisions of *Regulation 2018/302/EU of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC* entered into force. (OJ L 60, 02.03.2018, p. I/1), commonly referred to as the Geoblocking Regulation. However, the catalogue of exemptions to the Regulation includes financial services (banking, credit activities, insurance) which can be offered in different options according to their origin. Thus, mobile payment services offered by an operator from one jurisdiction may be directed to a user from another jurisdiction. This poses a certain risk of money laundering or financing of terrorism, given that the services of a mobile payment operator may originate from a country with a weak anti-money laundering and counter-financing of terrorism system.

580. The risk factor for mobile payments is the fact that mobile payment services enable account and transaction financing in various ways. The majority of mobile payment services are based on the banking model, i.e. connecting funds from a bank account or payment card. However, some mobile payment services do not use the banking model and the virtual purse can be recharged by other means, e.g. *online*, even from an unidentified counterparty. Such possibilities for financing of a virtual purse obscure the origin of the funds, creating a higher risk of money laundering and financing of terrorism.

581. Using mobile payment services, users have access to cash through an international network of ATMs. Such access to cash increases the level of risk of money laundering and financing of terrorism by allowing the transfer of money in one country and their withdrawal in another country.

---

[264] Guidance for a risk based-approach, prepaid cards, mobile payments and internet-based payment services, FATF, June 2013, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html.

Gambling

582. Article 3(14) of Directive 2015/849 introduces a definition of "gambling services". According to it, the term includes a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.

583. In accordance with the provisions of Article 2(1) of the *Act of 19 November 2009 - gambling law*, games of chance are games, including those arranged online, where the prize is either cash or a material prize and where the result depends primarily on chance. Games of chance are games, including those arranged online, where the prize is either cash or a material prize and where the result depends primarily on chance. They include: number games, cash lotteries, telebingo, cylindrical games, dice games, cash bingo game, raffle bingo game, raffle lotteries, promotional lotteries, audiotele lotteries.[265]

584. Betting means betting for cash or material prizes based on guessing:

- the results of a sports competition in which competitors are people or animals and

  where the participants pay stakes, while the prize depends on the total amount of stakes paid – sweepstake systems;
- occurrence of various events, including virtual events, in which participants pay their stakes, and the amount of winnings depends on the agreed, between the person accepting the bet and the person paying the stake, ratio of payment to win - bookmaking.

585. Virtual events shall be computer-generated events related to sports competition of people or animals.

586. Card games include such games as: black jack, poker and baccarat, as long as they are played in order to win cash or material prizes.

587. Games on gaming machines mean:

- games played with the use of mechanical, electromechanical or electronic devices, including computer hardware and games corresponding to the rules of games on gaming machines arranged via Internet, where the prizes are either cash or material prizes and where the game contains an element of a lottery;
- games played with the use of

  mechanical, electromechanical or electronic devices, including computer hardware and games corresponding to the rules of games on gaming machines arranged via Internet for commercial purposes, in which a player has no possibility to win cash or material prizes but the game has features of a lottery.

588. The recitals to Directive 2015/849 imply that it is highly probable that the gambling sector will be used to legalise criminal proceeds. In its supranational assessment of the risks of money

[265] https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/, date of reading 21 May 2019

laundering and financing of terrorism, the European Commission concluded that only some gambling products were considered to be significantly exposed to money laundering risks[266] In the case of stationary betting and poker services, the risk of money laundering and financing of terrorism stems in particular from ineffective controls. The document explains that services in the scope of betting and poker (stationary) by their very nature involve a significant number of quick and anonymous transactions, often in cash or with a P2P payment element, which, in the absence of adequate supervision, can generate high risks.

589. In the transnational assessment of the risk of money laundering and financing of terrorism, much attention has been paid to *online* gambling, where a high exposure occurs to risk resulting from the large number of transactions / financial flows and their indirect nature. The reason for this conclusion is the fact that *online* gambling allows for anonymous payment methods, although they simultaneously offer an important risk mitigating element consisting in tracking transactions. Recognising this problem in Poland, the KAS cooperates with the KNF (PFSA) in the scope of enforcement of the prohibition to act as an intermediary in payments for participation in gambling games arranged via the Internet on the territory of the Republic of Poland to entities illegally arranging gambling games via the Internet. For example, as a result of the said cooperation, the KNF (PFSA) developed a position in which it included an instruction for payment service providers to cease, with an immediate effect, providing services to entities illegally arranging online gambling, and thus to cease violating the law in force in the territory of the Republic of Poland[267]

590. In the Polish system a considerable risk exists in the area of tax crime related to gambling on gaming machines. Since 1 January 2010, when the provisions of *the Act of 19 November 2009 - Gambling law* entered into force, the installation and operation of gambling machines has been limited to casinos only. In the period before the Act in question came into force, the gaming machines had also operated outside casinos on the basis of licences which were gradually phased out during the transitional period following the entry into force of the Act in question. The transitional period during which the authorisations granted in the previous period expired lasted until 18 December 2015. However, many gaming machine owners do not comply with the applicable legislation and operate outside the casinos in the shadow economy. The operation of premises which are not casinos where gaming machine services are offered is subject to control by the KAS bodies. These bodies distinguish three types of shadow economy activities related to gaming machines, i.e.:

- arranging games without a licence on traditional (classic) gaming machines,
- arranging illegal games with the use of terminals (Internet kiosks),
- arranging illegal games on simulators.

591. According to the data derived from the report of the Head of the National Revenue Administration for 2018, as a result of measures undertaken by the KAS bodies in the scope of

[266] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 152-183 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[267] https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_ws_posrednictwa_dostawcow_platniczych_w_platnosciach_za_gry_hazardowe_w_Internecie_48077.pdf, date of reading 21 May 2019

control of gambling games and combating fiscal offence in the area of arranging games on gaming machines without a licence and unauthorised possession of gaming machines, in 2018 the KAS bodies carried out 2,963 inspections, as a result of which infringements of the binding regulations were found and the total of 10,956 illegal gaming machines were seized. In addition, more than 20,000 activities were undertaken by the KAS bodies to verify the sites where illegal arranging of games on gaming machines had been previously identified or, according to the information available, a probability of their occurrence was probable.

592. On 1 April 2017, an amendment to the *Act of 19 November 2009 - Gambling law* came into force, whose purpose was, among other things, to regulate the situation of games on gaming machines. As a result of this amendment, Totalizator Sportowy, the owner of the LOTTO brand, which is a state-owned company, manages games on gaming machines. In this way, Totalizator Sportowy exercises the state monopoly in this area. The first pilot game arcades for games on gaming machines owned by Totalizator Sportowy were launched in 2018. According to the latest information of the Ministry of Finance of April 2019, Totalizator Sportowy has 31 operating game arcades for games on gaming machines.

593. In the context of gambling games for the arrangement of which the licence or the concession is granted by the minister competent for public finance, in the segment of games organised in casinos, game arcades for games on gaming machines, betting points, the last report published by the Ministry of Finance - *Information on the implementation of the Gambling Law in 2017*[268] shows that at the end of 2017, 49 casinos operated in Poland, 28 companies operated the total of 2,510 betting points and 7 licences for the arrangement of betting via the Internet were in force. Poker tournaments could have been held only in casinos until 31 March 2017 and the competent authority for authorising such tournaments was the minister competent for public finance. Operators of casinos under the license granted had a possibility to apply for a license in this scope. In 2017, 4 licences for arranging poker tournaments were granted to 2 entities holding licences to operate casinos. On the other hand, as of 1 April 2017 - following the amendment of *the Act of 19 November 2009 - Gambling law* , the minister competent for public finance has ceased to grant any permits for the arrangement of poker tournaments. A poker tournament can be arranged outside the casino subject to notifying the director of the revenue administration regional office competent for the venue of the tournament of such a tournament and after fulfilling the terms and conditions defined in the provisions of the Law. On the other hand, in accordance with the provisions of the Gabling Act, the arrangement of promotional lotteries, audiotele lotteries, raffle lotteries and bingo games is subject to the obligation to obtain a licence from the competent director of the revenue administration regional office.

594. In terms of the sector, casinos are inherently highly exposed to risk. It is mainly associated with the purchase and repurchase of tokens (e.g. for cash or by means of anonymised products). Criminals may use substituted persons who buy tokens for cash and then pass them on to the perpetrator pretending that they come from the winning. In addition, casino games may be used

[268]https://www.podatki.gov.pl/media/3011/informacja-o-realizacji-ustawy-o-grach-hazardowych-w-2017-roku.pdf, date of reading 21 May 2019

where co-operating players lose/win similar amounts (for example, one "bets on red" while the other "bets on black" when playing the roulette)[269]

595. An important problem in the gambling sector is the risk of infiltration or taking over the ownership of gambling and betting operators by organised criminal groups.

Activities of non-profit organisations

596. Recognising of *non-profit* activities as a risk area for abuse for the needs of money laundering or financing of terrorism is linked to the recommendations of the FATF. In Recommendation No. 8 the FATF indicated that individual countries should make every effort to ensure that such *non-profit* organisations (NPOs) are not used for money laundering or financing of terrorism purposes.

597. In accordance with the FATF definition, the NPO shall mean a legal person or a legal arrangement, or an organisation that is engaged primarily in raising or distributing funds for charitable, religious, cultural, educational, social or fraternal purposes or to carry out other types of "good work"[270]

598. The European Commission has specified the scope of NPO activity in more detail, indicating that it comprises:

- "service activities" which include programs focusing on the provision of housing, social services, education or health care (for example, it may involve the provision of humanitarian or development aid, as well as other conducting other types of activities);
- "expressive activities", i.e. programs focusing on sport and recreation, arts and culture, representation of interests or support, pursued for example by political parties, *think tanks* and advocacy groups (i.e. organisations generally engaged in philanthropic activities)[271]

599. On the basis of Polish law, such organisations include first of all foundations, as well as all kinds of associations. Pursuant to Article 3(2) of the *Act of 24 April 2003 on public benefit activity and volunteering*, foundations and associations are classified as NGOs [272] and as such are subject to the regulations of this Act, thus having the possibility to apply for the status of a public benefit organisation or benefit from subsidies from public administration.

---

[269] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 163-166 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[270] Best practices - Combating the abuse of non-profit organisations (Recommendation 8), FATF, June 2015, p. 7, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html.

[271] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, p. 185 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[272] With some exceptions indicated in Article 3(4) of *the Act on public benefit activity and volunteering.* One of them is a foundation established by political parties.

600. However, not all of these entities generate a similar risk of being used for money laundering. Low risk of money laundering is associated with the activities of such entities as voluntary fire brigades, operating under the provisions of *the Act of 7 April 1989 - Law on Associations* and the *Act of 24 August 1991 on fire protection* (Journal of Laws of 2018, item 620 as amended). Some of them have been included in the National Rescue and Firefighting System (KSRG) of the state security[273]

601. NPOs usually enjoy public trust. Moreover, they have access to substantial and diversified sources of financing, often in cash form. Their transactions are sometimes international in nature, especially for organisations operating in several or more countries where they may have establishments or branches.

602. According to the European Commission's assessment, the possible scenarios related to the collection and transfer of funds through the NPO can be as follows:

- establishment of a NPO in order to "raise funds" - funds from criminal activity are gradually transferred to this organisation (such an organisation may be used to support a specific criminal group or terrorist organisation by the so-called "outsiders", i.e. persons from outside the NPO or by the so-called "insiders", i.e. persons operating within the NPO);
- using existing NPOs to finance local terrorist activities or facilitate execution of international transactions to transfer funds to areas where NPOs operate close to terrorist areas (in this case, the organisation may also be used to support a particular terrorist organisation or criminal group, by so-called "outsiders" or "insiders")[274]

603. The European Commission has assessed the threat of money laundering in the area of NPO activities in the context of the risk of financing of terrorism, i.e. using *modus operandi* related to the collection and transfer of funds in order to finance terrorist activities.

604. However, the experience of the GIFI shows that NPOs can also be used for money laundering without any links to terrorist organisations and financing of terrorism. The threat of using NPOs for money laundering is based primarily on attributes of their activities, such as:

- execution of transactions with many entities - natural persons and legal entities (including accepting cash from both regular and accidental one-time donors);
- using methods of raising money to facilitate the concealment of their origin and the identity of actual donors (e.g. public collections, charity auctions);
- numerous types of transactions, both cash and non-cash, sometimes of an international nature.

---

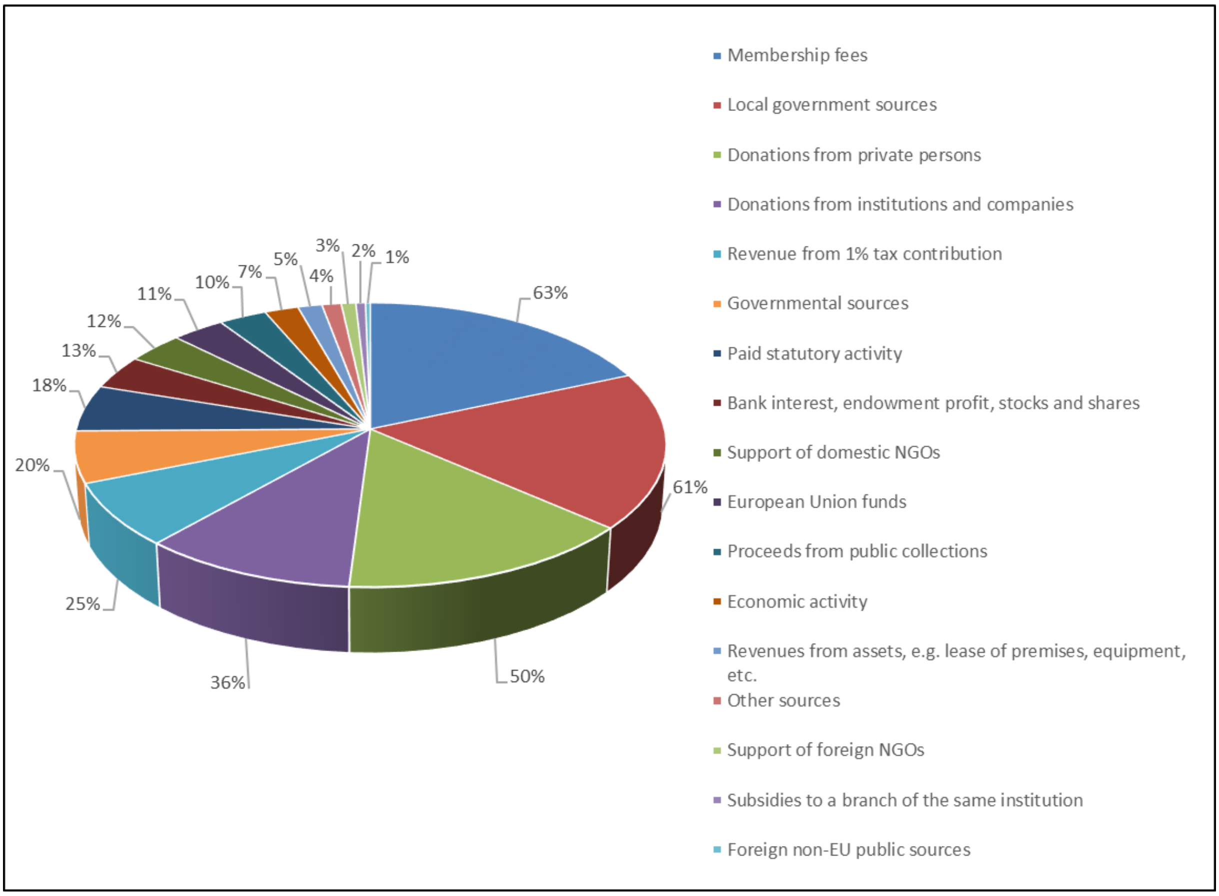
[273] "As of July 2018, 4,404 OSP units are included in the KSRG. In addition, there nearly 12,000 non-system units also operate in the KSRG." (see: https://www.gov.pl/web/mswia/ochotnicze-straze-pozarne, date of reading 21May 2019

[274] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 185-186 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

605. Foundations and associations can obtain funding from a variety of sources, among others, from:

- subsidies;
- paid public benefit activity;
- economic activity, selling services or products in exchange for the implementation of statutory purposes (in this case they are obliged to register their business activity);
- public collections;
- cash donations and gifts in kind;
- sponsorship;
- charity auctions.

Figure no. 14 - Percentage of organisations (associations and foundations) using individual sources of income in 2017[275]



[275] Based on the data derived from: 2018 - Condition of NGOs, Klon/Jawor Association, Warsaw, February 2019, p. 40, available at: https://fakty.ngo.pl/raporty/kondycja-organizacji-pozarzadowych-2018.

606. The above mentioned data show that more than half of the organisations used membership fees and/or self-government sources and donations from private persons in 2017.

Table no. 22 - Percentage of organisations (associations and foundations) using individual sources of income in 2017[276]

Number of fund types in the budget	Percentage of organisations	Average revenues in 2017
no more than 3	53%	PLN 13 thous.
4-6	35%	PLN 55 thous.
6-9	9%	PLN 129 thous.
10 and more	2%	PLN 1.7 million

607. A considerable part of the NPOs uses various sources of fund-raising. According to the analysis carried out by Klon/Jawor, the higher their number, the higher the average income. Although the number of NPOs with relatively high average revenues (exceeding one million PLN) and many sources of revenues is relatively small (2% of organisations with average revenues at a level of PLN 1.7 million).

608. Numerous fund-raising sources make it possible to transfer assets from illegal activities to the NPOs for laundering. For example, cash acquired as a result of crime, contributed by straw men or non-existing natural or legal persons can then legally be transferred to specific individuals or economic operators, in accordance with the purposes indicated in the organisation's statutes.

609. Among the analytical proceedings instituted by the GIFI in 2016-2018 there was a relatively small percentage of such proceedings in which entities with the words "association" or "foundation" in their names were registered (approx. 1.2% of all analytical proceedings). Similar percentage was also recorded for analytical proceedings in which notifications were sent to the prosecutor's office in 2016-2018 and in which entities with the word "association" or "foundation" in their names were registered, in relation to all analytical proceedings in which notifications were sent to the prosecutor's office in connection with the suspicion of money laundering (i.e. approximately 1.2%). However, already looking at the data for 2018 only, it can be observed that they are respectively higher (i.e. about 1.7% in the case of for analytical proceedings initiated in 2018 and about 2.6% for analytical proceedings in which notifications were sent to the prosecutor's office in 2018)[277]

610. One of the analytical investigations in which the notification was sent to the prosecutor's office concerned suspicion of money laundering from the illegal trade in medicines. Entities participating in this procedure also included a *non-profit* organisation. In other analytical proceedings, the GIFI submitted notifications to the prosecutor's office concerning the suspicion of laundering money from tax fraud and extortion of significant amounts of money from natural and legal persons. Usually, foundations established and/or controlled by criminals were used for this purpose.

[276] Ibidem, p. 39.
[277] According to the information registered in the GIFI IT system by 21 May 2019.

Trading in high value commodities / goods

611. The possibility of using high-value or luxury goods for money laundering has been highlighted by various international organisations. In the FATF recommendations, the role of trading in precious stones and metals in this area is emphasised. On the other hand, *Transparency International*, on the other hand, draws attention to the risks associated with the possibility of using luxury goods for money laundering. In addition to precious stones and metals, the category of luxury goods includes works of art, super-yachts, personal luxury items (i.e. high-end clothing, footwear, watches, perfumes, etc.) as well as real estate[278]

612. Legal regulations of some countries impose specific anti-money laundering and counter-financing of terrorism obligations on traders in high-value goods/commodities. An example is the German law in this area – *Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen (vom 23. Juni 2017).* It defines objects that differ from everyday utility objects by their properties, designation or market value or are distinguished from everyday acquisitions by their price as high-value goods/commodities. They include, first of all:

- precious metals such as gold, silver, platinum;
- precious stones;
- jewellery and watches;
- works of art and antiques;
- cars, ships, motorboats and aircrafts[279]

613. In its transnational assessment of the risk of money laundering and financing of terrorism, the European Commission has paid particular attention to trading in works of art and antiques. As a basic *modus operandi* of criminals, it indicated the conversion of funds originating from criminal activity into antiques and works of art to make it easier to store or move assets of this kind[280]

---

[278] Tainted Treasures Money laundering risks in luxury markets, ed. Transparency International, 2017, available at:https://www.transparency.org/whatwedo/publication/tainted_treasures_money_laundering_risks_in_luxury_markets.

[279] § 1 (10) *Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen (vom 23. Juni 2017)*: "Hochwertige Güter im Sinne dieses Gesetzes sind Gegenstände,
1. die sich aufgrund ihrer Beschaffenheit, ihres Verkehrswertes oder ihres bestimmungsgemäßen Gebrauchs von Gebrauchsgegenständen des Alltags abheben oder
2. die aufgrund ihres Preises keine Alltagsanschaffung darstellen.
Zu ihnen gehören insbesondere
1. Edelmetalle wie Gold, Silber und Platin,
2. Edelsteine,
3. Schmuck und Uhren,
4. Kunstgegenstände und Antiquitäten,
5. Kraftfahrzeuge, Schiffe und Motorboote sowie Luftfahrzeuge."

[280] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, p. 124 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

614. The European Commission also indicated that cases of trading in stolen cultural goods (artefacts and antiques) within the EU had been identified. Member States conducted a number of investigations/proceedings concerning trade in stolen artefacts and antiques originating from conflict areas, such as Iraq and Syria (where Far East countries were used to facilitate the concealment of stolen goods). Moreover, the studies performed show that the main threats in this area include plundering of cultural goods (artefacts and antiques) in third countries (especially in conflict areas such as Syria) and the procedure related to imposing taxes on such activities by terrorist organisations controlling the particular territory. For example, the source of funding for the so-called Islamic States of Iraq and Sham (ISIS) was not the sale of stolen cultural goods but income gained from the sale of excavation permits and transit fees. The cases identified in this risk area show that terrorists do not sell stolen cultural goods to raise finance. Robbed cultural goods can be sold in the EU through intermediaries and an indirect risk of financing of terrorism exists.

615. According to the European Commission, the use of the above *modus operandi* may be profitable, however, it is not easy to apply as it requires access to the illegal market. In addition, it is also a necessary requirement to have adequate technical knowledge as well as knowledge of the art market. The transport of stolen cultural goods is also not sufficiently safe.

616. However, the above scenario could be of interest to organised criminal groups as a means to convert funds from various offences or evasion of tax on cultural goods. However, such practices flourish mainly in free trade zones (i.e. duty free zones and so-called *free ports*) which makes it much more difficult to measure the real scale of this phenomenon.[281]

617. In Poland, the trade in cultural goods is regulated, among others, by *the Act of 23 July 2003 on the protection and care over historical monuments* (Journal of Laws of 2018, item 2067, as amended), *the Act of 25 May 2017 on restitution of national cultural property* (Journal of Laws of 2017 item 1086, as amended), *Regulation of the Minister of Culture and National Heritage of 4 December 2017 on the registration books kept by business entities specialising in the trade in monuments within the territory of the Republic of Poland* (Journal of Laws of 2017 item 2249, as amended), as well as international agreements.

618. In the context of combating crime in Poland, works of art and antiques usually appear in connection with counterfeiting or theft. Among others, Poland took part - together with 21 other countries and the World Customs Organisation - in an operation initiated by Interpol and Europol aimed at combating theft and illegal trade in cultural goods, including, in particular, illegal trade in monuments on the Internet. It was conducted from 22 to 31 October 2018 (its preparation within the initial phase started already on 20 September 2018). During the operation, the focus was on revealing cases of theft of cultural heritage in land and underwater areas, illegal trade in cultural goods - with special attention to conflict countries as well as theft of historical monuments. Another important objective was to gather information on persons or criminal groups illegally exploring archaeological sites and committing crimes against cultural goods[282]

619. As a result of the conducted action, several people associated with illegal trade in cultural goods were detained. Moreover, about 3,480 objects were recovered (including valuable

[281] Ibidem pp. 124-125.
[282] http://www.policja.pl/pol/aktualnosci/166389,Dzialania-w-ramach-miedzynarodowej-operacji-wymierzonej-w-zwalczanie-kradziezy-i.html , date of reading 23 May 2019

archaeological monuments excavated by means of metal detectors), including several old prints and a valuable painting monument stolen in Sweden in 2015. On the basis of the materials collected during the operation, 26 new preparatory proceedings were instituted.

620. In addition, on 20 - 30 November 2017, the Polish Police, together with police and customs authorities from 21 EU Member States, took part in the operation under the code name Pandora II, coordinated by Europol. Its main objective was to combat theft and illegal trade in cultural goods (in particular via the Internet)[283]

621. As a result of the activities of the Polish Police - cooperating with, among others, the KAS and the Border Guard[284] - several people associated with illegal trade in cultural goods were detained in our country, 24 new proceedings were instituted and 3,629 cultural goods were secured, almost half of which are archaeological monuments.

622. According to the European Commission, assets originating from illegal activities can be transferred to another country to buy diamonds, gold or jewellery and such assets are subsequently sold in a third country on the basis of false invoices and certificates, or used directly to buy gold on the territory of the specific, then sold to metal brokers, who will then resell it to other companies. The proceeds of the sale may then be transferred to a third party to finance new criminal activities. The European Commission's assessment shows that precious metals and stones (usually gold and diamonds) are most popular among criminal organisations as they are easy to store and exchange for a small fee[285]

623. In Poland, imports, processing and marketing of diamonds is not a legally regulated activity, which means that it does not require a licence, a concession or any other decision of a public administration authority. In order to ensure that the diamonds purchased are natural and come from legal sources, buyers may use services of certain partners offering internationally recognised certificates attesting the legal origin of the stones. Each diamond must have an expert certificate that guarantees the authenticity of the stone (the value of the stone will additionally increase if the certificate is issued by one of the independent international gemological laboratories).

624. Precious metals are traditionally considered as a particularly good way to invest funds. In Poland, it is possible to buy gold in the form of bars as well as gold coins - so-called bouillon coins (without numismatic values). An additional advantage of the bouillon coin is its classification as a legal means of payment, which ensures a possibility of its transport from country to country. Gold bars and gold coins can be purchased without any major problems from banks or independent gold distributors. Investment gold[286] and bouillon coins can also be

---

[283]http://policja.pl/pol/aktualnosci/156014,Dzialania-polskiej-Policji-w-ramach-Miedzynarodowej-Operacji-PANDORA-II.html , date of reading 06 June 2019

[284] Also with the Ministry of Culture and National Heritage and the National Heritage Institute, the National Institute of Museums and Collections Protection, Regional Offices for Monument Protection and the Polish Episcopal Conference.

[285] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp.129 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[286] In accordance with Article 1 of *the Act of 11 March 2004 on value added tax* (Journal of Laws of 2018 item 2174 as amended), the term investment gold shall be construed as: “1) gold in the form of bars or wafers of a purity

purchased at the mint. The largest mint in Poland is the Mint of Poland. However, it is not accredited by the London Bullion Market Association, therefore the gold bars of the Mint of Poland can only be sold at the NBP or at local gold buying points.

625. Also some other goods of high value, such as cars, jewellery, watches, luxury boats can be attractive to criminals. Criminal groups can use such products as an easy way to integrate criminal funds into legitimate financial resources, transforming criminal proceeds into assets that retain their value, and the market price of some of them may even rise over time.

626. The KPMG Sp. z o.o. report on the Polish luxury goods market in 2018 has defined luxury goods as any good (including services) bearing a brand commonly recognised as luxury brand on a given market or which, due to its specific nature (uniqueness, high price, etc.) acquires a luxurious character. Based on this definition, this category includes products and services from such categories as: cars, clothing and accessories, real estate, alcohols, hotel and SPA services, jewellery and watches, cosmetics and perfumes as well as yachts and aircrafts[287]

627. According to the above-mentioned report of KPMG Sp. z o.o., the largest segment of luxury goods are *premium* cars and luxury cars. According to the estimates presented in the report, the value of this market in 2018 could amount to approximately PLN 15.5 billion and the number of registrations of new cars belonging to *premium* brands could amount to 76,259 pcs. and in the case of luxury brands - to 251 pcs.[288]

628. The second largest segment of luxury goods in Poland is the segment of luxury clothing and accessories. The value of the market of luxury clothing and accessories in 2018 was estimated at almost PLN 2.9 billion (i.e. 7.2% more than in 2017). Women's clothing has the major share in the segment with its value constituting approx. 61% of the entire category, however, men's clothing achieved a higher growth[289]

629. The sector of luxury jewellery and watches is growing very dynamically. More than 80% of luxury watches available on the market is designated for men and 67% of luxury jewellery is addressed for women. The value of the market of luxury jewellery and watches may amount to approximately PLN 723 million in 2018, of which jewellery constituted over 60%.[290]

630. On the other hand, the value of the market of luxury spirits in 2018 could reach PLN 1.2 billion. The market of luxury alcohols comprises spirits whose share is estimated at 72% as well as wines and champagnes. About 62% of the share in the entire segment is held by whisk(e)y which demonstrates the highest growth dynamics among all luxury alcohols (the value of its sales increased by 11% as compared to 2017)[291]

---

of at least 995 thousandths, and gold represented by securities; 2) gold coins which jointly meet the following conditions:
a) have a sample of at least 900 thousandths,
b) were struck after 1800,
c) are or were a legal tender in the country of origin,
d) are sold at a price which does not exceed the market value of the gold contained in the coin by more than 80%."

[287] Luxury Goods Market in Poland - Edition 2018, KPMG, 2018, available at: https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/11/pl-Rynek-dobr-luksusowych-w-Polsce-2018.PDF.

[288]Ibidem, p. 20.

[289]Ibidem, p. 24.

[290] Luxury Goods Market in Poland - Edition 2018, KPMG, 2018, p. 40, available at: https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/11/pl-Rynek-dobr-luksusowych-w-Polsce-2018.PDF

[291]Ibidem, p. 32.

631. Year by year, the number of produced luxury yacht models is growing. Polish shipyards specialise in yachts up to 9 meters long. Poland is the leader in Europe and occupies the second place in the world just after the USA in terms of the number of yachts produced. However, due to the high price, the demand for luxury yachts in Poland is insignificant, they are mainly intended for export (predominantly to the USA, Western European countries, Russia and the Middle East)[292]

632. According to the Civil Aviation Office, there are 1,305 aircraft and 221 helicopters registered in Poland for natural persons and companies. Aircraft is an expensive investment, therefore the number of private aircraft is quite small. The majority of newly registered aircraft and helicopters are owned by companies - more than 81%. Despite the high price, the number of new registrations is increasing year on year. Compared to 2017, there were 49 more aircraft and 70 more in comparison with 2016. Private aircraft is considered as one of the most luxurious goods[293]

633. Information concerning the preparatory proceedings conducted in Poland (concerning both such predicate offences for money laundering as tax fraud as well as others, e.g. scamming loans/subsidies from the EU or drug smuggling and trafficking) often contains information that as a result of the performed activities, luxury cars as well as other high-value goods / commodities were seized.[294]

Real estate trade

634. The real estate sector is one of the areas used by criminal organisations for the purpose of laundering illicitly acquired funds. This sector has many features which make it attractive for the money laundering and financing of terrorism practice. In principle, the real estate market is international, geographically divided and numerous factors shape the local real estate price. The price of real estate at a given place and time is affected by many underlying factors for the due valuation of a given property market. Money laundering transactions in the particular real estate market can be easily concealed in real commercial transactions among a huge number of transactions related to real property. A significant factor affecting the complexity of detecting suspicious transactions in this market is the fact that often - especially in countries defined as developing markets - there is lack of relevant information (e.g. statistical data on the average market price of real estate) that can serve as a benchmark for determining the economic rationale for property purchase transactions.

635. Suspicious real estate transactions can also have undesirable political consequences, affecting the institutional and economic destabilisation of such countries. Due to the international nature of the real estate market, it is often very difficult to distinguish true real estate transactions from those related to money laundering or financing of terrorism. The inflow of financial resources to the specific country, triggering changes in real estate prices, may have a significant impact on investment decisions taken by potential purchasers and sellers of real

---

[292]Ibidem, p. 48.
[293] Luxury Goods Market in Poland - Edition 2018, KPMG, 2018, p. 52, available at: https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/11/pl-Rynek-dobr-luksusowych-w-Polsce-2018.PDF
[294]For example: http://www.policja.pl/pol/aktualnosci/167474,Rozbita-zorganizowana-grupa-wyludzali-podatek-VAT.html,http://www.policja.pl/pol/aktualnosci/173163,Wprowadzali-do-obrotu-nielegalne-paliwa-straty-Skarbu-wyniosly-44-mln-zl.html, http://www.cbsp.policja.pl/cbs/aktualnosci/167026,Mogli-wyludzic-ponad-68-mln-zl-z-funduszu-UE.html, http://policja.pl/pol/aktualnosci/173762,Podejrzani-mogli-wyprac-680-mln-euro-operacja-Lodolamacz.html – date of reading 23 May 2019

estate. Fluctuations in real estate prices can, in turn, affect individuals deciding where to live and work. They also have an impact on investment decisions made by state and local government bodies. Real estate prices can also have a significant impact on the construction industry, determining its development or stagnation. Taken together, all these factors suggest that price fluctuations in the real estate market, the development or stagnation of the construction industry, have a major impact on the economic activity and development of a country.

636. According to the information provided by Savills plc. - one of the best known companies providing global services in the sector of real estate trade listed on the London Stock Exchange - the global real estate market accounts for approximately 60% of all existing investment assets. The aforementioned company estimated the total value of global real estate assets in 2015 at approximately USD 217 trillion[295]. The value of the global real estate market in 2015 was 2.7 times higher than the global GDP. Real estate is an important element of national, corporate and private property. Residential properties accounted for approximately 75% of the global real estate market value. According to Savills plc. the largest and most important part of the global real estate market is the residential property market with the value of approximately USD 162 trillion. This sector demonstrates the most extensive dispersion of the ownership structure which covers about 2.5 billion households and is closely related to the wealth of average citizens. The value of residential property corresponds to the degree of prosperity of the society: China, with almost one fifth of the world's population, owns about one quarter of the market value. The value of assets is mainly concentrated in countries of the West. More than one fifth (21%) of the market is occupied by residential property located in North America, although only 5% of the world's population lives there. On the other hand, in the commercial real estate sector, North America accounts for almost half of the market. Europe accounts for more than a quarter, whereas Asia and Australasia - for 22%. In terms of the real estate estimation methodology, Savills plc. did not take into account small local commercial properties such as workshops, studios, shops and premises used by small businesses. In 2015, the value of global agricultural and forestry land was also estimated. This estimate amounted to approximately USD 26 trillion, of which approximately 30% of agricultural and forestry land is owned by corporations and institutional investors. Most of the agricultural and forestry land is owned by entities that do not invest but only exploit it.

637. For the use of the real estate sector in money laundering and financing of terrorism, a variety of methods, techniques, mechanisms and instruments are available. Most of these methods are illegal as such, but some of them may be considered legitimate if they were not carried out with the intention of money laundering or financing of terrorism (or if the link could not have been detected). There is also a wide variety of possible types of transactions that may be linked to money laundering or financing of terrorism in the case of the real estate sector. Nevertheless, this does not mean that all transactions that do not have sufficiently strong economic rationale are necessarily associated with illegal activities resulting in money laundering or financing of terrorism. It should be remembered that money laundering is always intended to hide it as a "normal" transaction. The criminal nature of real estate activity results from the origin of the funds used and the purpose of the transaction participants. Among the typologies included in the 2007 FATF report entitled: "Money laundering & financing of

[295] http://www.savills.pl/_news/article/0/198715-0/1/2016/%C5%9Bwiatowy-rynek-nieruchomo%C5%9Bci-stanowi-60--wszystkich-aktywow-inwestycyjnych, date of reading 22 May, 2019

terrorism through the real estate sector"[296], several basic methods of money laundering and financing of terrorism are mentioned. These include: the use of complex loans or credit financing, the use of intermediaries in the real estate market and other legal professionals, use of corporate vehicles, manipulation of property estimation or appraisal, use of monetary instruments, use of debt schemes, use of investment programs and financial institutions, use of real estate to hide money generated by illegal activities.

638. In real estate transactions, a number of common features can be identified which, individually or in combination, may indicate a potential use of the real estate sector for money laundering and financing of terrorism purposes. The real estate transaction itself often seems legal but some of the subjective or objective premises occurring within such transaction may indicate a link with money laundering or financing of terrorism. The criminal nature of such transactions results from the origin of the funds and the purpose for which they are carried out by the participants. The main factors increasing the risk of money laundering and financing of terrorism in the real estate market include the following circumstances:

- where the transaction involves a resident or an entity established in a high-risk country (e.g. tax havens);
- where it appears, on the basis of the conducted analysis process, that persons or firms do not have the economic capacity to undertake a real estate transaction, or where the amount of the transaction is disproportionate to the reported assets of the transaction participant;
- where transactions are carried out by persons linked (directly or indirectly) to criminal activities;
- transactions involving persons with business, family or social ties;
- transactions in which a large credit, a mortgage loan or a loan is repaid quickly - especially when the repayment is made in cash;
- transactions in which there is no connection between the transaction and the activity carried out by the acquiring company or in which the company does not carry on any economic activity;
- transactions where there is no economic justification or where there is an obvious loss for one of the parties to the transaction;
- transactions where, on the basis of an analysis carried out, there is a reason to believe that the parties to the transaction do not act on their own behalf but try to conceal the identity of the real customer;
- transactions where payments are made in cash or in other negotiable instruments which do not specify the real payer;
- transactions where the means of payment used to conclude the transaction originate in so-called higher-risk countries;

[296] Money laundering & terrorist financing through the real estate sector, FATF, 29 June 2007, available at:https://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingandterroristfinancingthroughtherealestatesector.html.

- transactions in which the acquisition and disposal of real property takes place in a short period of time and which involve a significant increase or decrease in price compared to the purchase price;
- transactions concluded at a value significantly different (much higher or much lower) from the real value of the real property or significantly different from the market value.

639. According to the report published by the GUS in November 2018 entitled: "Real estate trade in 2017" [297] prepared with the use of notarial reporting conducted by the Ministry of Justice, in 2017, 488.1 thousand of notarial deeds concerning the sale of real estate were signed in Poland, i. e. 1.2% more than the year before. Compared to 2016, the highest increase in the number of notarial deeds occurred in the case of sale of plots of land developed with residential buildings (by 7.5%), sale of apartments (by 7.4%), sale of undeveloped plots of land (by 4.9%) and sale of cooperative ownership right to premises (by 4.3%). The highest decline was recorded in the case of notarial deeds concerning the sale of agricultural real estate (by 17.6%) and other real estate (by 16.8%).

640. The structure of notarial deeds concerning the sale of real estate in 2017 was dominated by the sale of premises which constituted 39.2%. Moreover, sale of undeveloped plots of land (19.4%), sale of agricultural real estate (11.8%), sale of plots of land developed with a residential building (9.8%) and sale of cooperative ownership right to premises had a considerable share (9.7%).

641. In addition to the report published by the GUS, the NBP also publishes quarterly reports concerning information on housing prices and situation on the residential and commercial real estate market in Poland in specific quarters of a given year, containing a synthetic description of the most important phenomena taking place on the residential and commercial real estate market in the largest cities in Poland[298] The NBP also prepares annual reports[299] providing interested business entities, including real estate market participants, with possibly complete, reliable and objective information concerning the situation on the residential and commercial real estate market in Poland. The annual report focuses on general trends and conclusions resulting from analyses of the residential and commercial real estate market and detailed statistical information is presented in charts and tables. The NBP presents more detailed information in a layout covering each of the sixteen markets of capital cities of the country provinces.

642. In addition, the NBP publishes the so-called database of residential property prices[300], which includes both offer and transaction prices for the sale and rental of apartments within the administrative boundaries of 16 capital cities of the provinces and Gdynia. In these cities, a significant part of the market trade is performed (prices include VAT).

643. Analysis of transaction prices and forecasts for the Polish residential real estate market under the name E-VALUER INDEX is prepared every year by Emmerson Evaluation Sp. z o.o. The report for 2017 states that low return on investments and uncertainty related to the

---

[297] https://stat.gov.pl/obszary-tematyczne/infrastruktura-komunalna-nieruchomosci/nieruchomosci-budynki-infrastruktura-komunalna/obrot-nieruchomosciami-w-2017-r-,4,15.html, date of reading 22 May 2019.
[298] https://www.nbp.pl/home.aspx?f=/publikacje/rynek_nieruchomosci/index2.html, date of reading 22 May 2019
[299] https://www.nbp.pl/home.aspx?f=/publikacje/rynek_nieruchomosci/index1.html, date of reading 22 May 2019
[300] https://www.nbp.pl/home.aspx?f=/publikacje/rynek_nieruchomosci/index2.html, date of reading 22 May 2019

effectiveness of other forms of investment still stimulate Poles to invest capital in the housing market. In 2016, it was one of the main factors shaping the market since most purchases of new apartments were performed for cash.[301] According to estimates, over 60% of all transactions in 2016 were cash purchases, whereas transactions involving mortgage loans accounted for less than 40% of total market turnover. The said report was prepared by Emmerson Evaluation on the basis of nearly 60,000 transactions which took place in 2016.

644. Taking into account the relatively high percentage of cash transactions on the real estate market in Poland, found in the Emmerson Evaluation Sp. z o.o. report, a very important information function in the field of anti-money laundering and counter-terrorism financing in real estate trading may be performed by transaction participants associating the parties to these transactions, namely, intermediaries, i.e. entrepreneurs pursuing business activity in the scope of real estate intermediation. The real estate intermediation itself is a paid performance of activities aimed at concluding contracts by other persons but due to the various scope of concluded intermediation agreements, the knowledge of the intermediary about details of the transaction may be very high. Due to the fact that the provision of real estate intermediation services is not a licensed profession but requires only civil liability insurance, there is no precise information concerning the number of real estate agents in Poland. The Central Register of KIGN Real Estate Administrators and KIGN Real Estate Agents[302] is maintained by the National Chamber of Real Estate Management - as of 22 May 2019 there are approximately 3,100 entries in the register but there is also the FPPRN National Register of Real Estate Managers[303] maintained by the Polish Real Estate Market Agreement Federation (available by way of telephone or e-mail information). Intermediaries in real estate trading are obligated institutions within the meaning of *the Act of 1 March 2018 on Counteracting Money Laundering and Financing of terrorism.*

645. In addition to real estate agents, legal professionals are involved in real estate transactions[304] The National Notary Council operates the ICT system called Notary Registers, within which the following registers operate: Inheritance Register, Notary Wills Register (NORT), Central Repository of Electronic Notary Deed Extracts (CREWAN), Register of Succession Administrators, Register of Users, Notary Statistical Registers.

646. Acquisition by a foreigner of the ownership right or the right of perpetual usufruct of real estate and the purchase or acquisition by a foreigner of shares or stocks in commercial companies established in the territory of Poland being owners or perpetual users of real estate

---

301 https://www.emmerson-evaluation.pl/wp-content/uploads/2018/01/E-VALUER-INDEX-2017.pdf, date of reading 22 May 2019

302 http://www.kign.pl/rejestr/ , date of reading 22 May 2019

303 https://pprn.pl/?page_id=13612 , date of reading 22 May 2019

304 Pursuant to Article 2(1)(13) and (14) of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*, notaries have been included in the category of obligated institutions - in the scope of activities performed in the form of a notarial deed, comprising, inter alia:

- transfer of the ownership of an asset, including sale, exchange or donation of movable property or real estate,
- concluding an agreement on distribution of the estate, dissolution of co-ownership, life annuity, annuity in exchange for the transfer of the ownership of a real estate and on distribution of jointly held properties,
- assignment of the cooperative ownership title, title to premises, perpetual usufruct title and alleged promise of a separate ownership of premises,

as well as advocates, legal advisers, foreign lawyers, tax advisers to the extent that they provide legal assistance or tax advice to the client concerning the purchase or sale of real estate, an enterprise or an organised part of an enterprise.

located in Poland requires a permit from the minister competent for internal affairs. In order to obtain a permit, a foreigner should submit an application for issuance of the permit. The acquisition of real estate and shares in companies which are owners or perpetual users of real estate in Poland by foreigners from the European Economic Area and the Swiss Confederation does not require a permit from the minister competent for internal affairs.

Creation and operation of business entities

647. According to the European Commission, relatively numerous risk scenarios have been identified with respect to the creation of business entities and their services, including the creation of complex structures by criminal groups, covering various jurisdictions (in particular *offshore* jurisdictions), with hidden ownership links, under which the beneficial owners of subsequent entities operating in these structures are located in countries other than those where these entities are registered[305] Individuals acting as representatives of established entities and formally responsible for them are only a cover for real beneficial owners. In this way, representatives of criminal groups can remain anonymous and introduce criminal assets into the legal economy.

648. In terms of costs, the creation of an economic operator or a legal arrangement is usually quite simple and in very many cases it can be performed *online*. Relatively higher costs or a higher level of knowledge and planning may be required if criminal organisations use intermediaries to create more complex/complicated organisational structures. Knowledge of national and international regulatory and tax regulations is also useful in such situations and can often be provided exclusively by professional intermediaries.

649. According to the FATF analysis, the extensive ownership structures created to conceal the real beneficial owners are mainly based on using companies that do not carry out any real economic activity or any other independent operations and do not have employees or any significant assets (so-called *shell companies)*. Moreover, operating companies with the characteristics of legal companies are also used to conceal and obscure illegal financial activity (so-called *front companies)* as well as bearer shares and stocks, although these forms are less popular[306]

650. The applied methods also use other possibilities, such as - apart from the so-called "straw men" - formally representing business entities - also other legal entities identified as directors of controlled business entities, trusts and other similar legal arrangements, as well as *shelf companies* (i.e. companies with inactive shareholders, directors and secretaries that remain dormant for a long period of time although customer relationships have already been established - sometimes these companies are recognised as *shell companies*) and intermediaries facilitating the establishment of these business entities[307] In addition, typically criminal methods related to falsifying the activities (e.g. the use of false documents) are also used.

[305] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, p. 107 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.
[306] Concealment of Beneficial Ownership, FATF, July 2018, p. 5, available at: https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html.
[307] Ibidem pp. 25-45.

651. The cases analysed by the FATF for the purposes of preparing the report entitled: "Concealment of Beneficial Ownership" show that among all types of intermediaries facilitating the establishment of business entities, services of entrepreneurs providing services for companies and trusts were most frequently used.[308] In analytical proceedings carried out by the GIFI (especially related to the suspicion of laundering money originating from tax offences), entities involved in suspicious financial flows often included economic operators set up and/or operated by such intermediaries. The fact that business entities created by such intermediaries could be used for criminal purposes was demonstrated by such indicators as: shareholders/owners are persons who are so-called "straw men" who are characterised by a lack of property or income, often without Polish citizenship; companies with the same registered office address and minimum share capital, registered by the same person in a relatively short period of time.

652. In Poland, pursuant to *the Act of 6 March 2018 - entrepreneur law* the principle of freedom of economic activity applies, which enables undertaking of any legally permitted venture. Only to perform economic activity in areas which are of particular importance for the security of the State or citizens or for other important public interests where such activity cannot be exercised as a free activity, an appropriate licence, authorisation or entry in the register of regulated activity shall be required. The Polish law recognised an entrepreneur as a natural person, a legal person or an organisational unit other than a legal person on whom a separate act confers legal capacity, performing business activity and partners in a civil partnership within the scope of their business activity. The business activity may be commenced on the day of filing an application for entry in the Central Registration and Information on Business or after entry into the Register of Entrepreneurs of the National Court Register, unless specific provisions provide otherwise. However, a capital company in an organisation may undertake business activity before being entered into the register of entrepreneurs.

653. According to data from the Central Economic Information Centre, about 1,000 companies are established in Poland every day. In the period from January to the end of February 2019, 63,508 companies launched their operations. In 2018, 377,885 launched their operations.[309]

654. Polish law provides for the possibility of conducting business activity in the following forms:

- sole proprietorship;
- civil partnership;
- partnerships: general partnership, partnership company, limited partnership, limited joint-stock partnership;
- capital companies: limited liability companies, joint stock companies.

Among commercial companies, the most popular is the limited liability company.

655. For several years now, some activities in Poland can also be registered via the Internet[310]

[308]Ibidem, p. 6.
[309] https://www.coig.com.pl/ , date of reading 10 May 2019
[310] It is also possible to register a sole proprietorship online. Since 2012, the provisions of the Commercial Companies Code enable the registration of a limited liability company via the Internet (so-called S24 mode). In 2015, the possibility of registering general partnerships and limited partnerships via the Internet was introduced

656. According to one of the Internet portals in Poland, anonymity is becoming more and more attractive among owners or managers of companies. There are several reasons for interest in this type of solutions, e.g. in many contracts of employment, commission, cooperation or other similar agreements, non-competition clauses are included. "This prohibition most often consists in the prohibition of participation in other capital companies, partnerships, prohibition of running a sole proprietorship or sitting on the board of directors. Non-competition clauses often do not prohibit the fiduciary holding of shares." [311]

Safe Deposit Boxes

657. In accordance with Article 5(2)(6) of *the Act of 29 August 1997 - Banking Law*, banking activities include providing access to a safe-deposit box, as long as that such activity is performed by banks. Other legal provisions also do not limit the subjective scope of such providing such a service. This means that safe deposit boxes may also be made available by other entities.

658. On the Internet, it is possible to find at least several offers from various private, non-banking companies offering the aforementioned service. In some cases, the provision of this service may be associated with the storage of certain types and sources of goods (e.g. mints trading in gold usually allow storage of only those valuable items that were purchased from them[312], one of the mints also advertises that it offers safe storage of the purchased gold and the fee depends on the amount of gold stored).

659. Sometimes access to safe-deposit boxes provided by private companies is relatively easier than in banks since they are available 24 hours a day all year round, although this is reflected in the fee for their use[313].

660. It is also worth mentioning that the services related to safe-deposit boxes in Poland is not only provided by companies registered in our country.

661. In the transnational risk assessment, the European Commission has stated that criminals use such services to raise larger sums of money, financial instruments or other valuable assets (awaiting their conversion to cash) before they are entered into the banking system.[314] Although the use of safe-deposit boxes may not seem financially attractive, it does allow for hiding the proceeds of crime.

(using templates of contracts made available by the Ministry of Justice). Applications for registration under this procedure are processed within one day. The moment of entering the data into the IT system is considered as the moment of concluding the articles of association. In order to establish a company via the Internet, it is required to have a qualified electronic signature or a signature confirmed by the e-PUAP trusted profile.

[311] http://doradcatransakcyjny.pl/anonimowosc-w-spolce-czyli-jak-zarzadzac-spolka-i-byc-anonimowym/ , date of reading 10 May 2019

[312] In a sock, in the garden, in the bank, in the private vault? Where and for how much gold and valuables can be stored?, 4 July 2018, available at: https://subiektywnieofinansach.pl/w-skarpecie-ogrodku-w-banku-w-prywatnym-skarbcu-gdzie-i-za-ile-mozna-przechowac-zloto-oraz-kosztownosci/.

[313] The amount of fees is also influenced by other factors, such as the size of the box or necessary insurance - Anna Zalewska, Why it is worth having gold, 31 October 2018, available at: https://www.analizy.pl/fundusze/temat-tygodnia/24432/dlaczego-warto-miec-zloto.html).

[314] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, p. 103 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

5.4. MOST COMMONLY USED MONEY LAUNDERING METHODS

662. In the aforementioned GIFI guide for obligated institutions and cooperating units "Counteracting money laundering and financing of terrorism" there is a description of about several dozen money laundering methods. Their major part concerned the use of specific products and services offered on the market, especially on the financial market (e.g. foreign exchange transactions, insurance policies, credits, loans, securities and securities accounts).

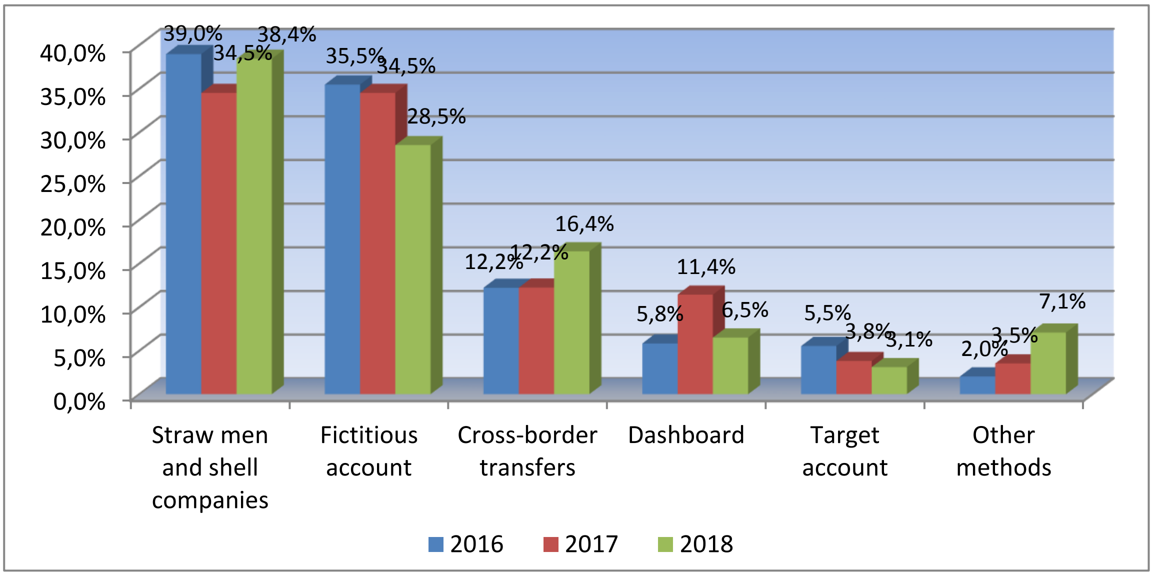
663. Some of the best known money laundering methods involve the use of bank accounts (as well as other payment accounts). They include:

- “fictitious account” (a method consisting in opening an account for the execution of one or more transactions, at short intervals, for very high amounts, using a maximum number of fictitious elements, e.g. forged documents presented at the opening of the account, providing a false purpose of opening the account or false purposes of the transactions ordered);
- “cross-border transfers” (a method that uses cash transfers to transfer property values between different jurisdictions);
- “dashboard” (a method based on crediting an account with deposits, often below the threshold requiring registration and coming from various sources in order to transfer funds held in the account to another account or accounts, including by electronic means, once the balance on the account has reached a sufficiently high level);
- “target account’ (a method of transferring large amounts of money to a single account - often of relatively short duration - from which they are immediately withdrawn in cash).

664. On the basis of the content of notifications to the public prosecutor's office on suspicion of money laundering, submitted by the GIFI in the years 2016-2017[315], it can be concluded that methods most frequently identified in the analytical proceedings conducted by the GIFI - apart from the method of “straw men and shell companies” - included such methods as ”fictitious account”, “cross-border transfers”, “dashboard’ and “target account”.

[315] It refers to the so-called main notifications. Besides them, the GIFI also provides the prosecution offices with the so-called supplementary notifications, following main notifications, containing materials connected in objective or subjective terms with the proceedings conducted by the prosecution offices in cases of money laundering, from which a reasonable suspicion of committing the said offence resulted.

Figure No. 15 - Percentage share of the identification of the use of particular money laundering methods in all the identification of money laundering methods on the basis of the content of the main notifications submitted by the GIFI in 2016-2018 to the public prosecutor's office in connection with a suspected money laundering offence



665. The “fictitious account” method is often used in cases associated with laundering money originating from VAT fraud. In such cases, bank accounts are set up to perform - in a relatively short period of time - financial transactions aimed at confirming the cash flow for the purchase of goods and, at the same time, making it more difficult to trace the money flow from unpaid VAT. Besides, the above method is also used to launder money coming from other types of offences.

666. The “dashboard” method enables introduction of funds from illegal sources into financed transactions and their rapid transfer to other places/locations. The example below illustrates the use of this method.

<u>Example no. 1.</u>

A foreign company pursued the procedure consisting in performing banking activities comprising accepting of cash contributions intended for investment in arts. Meetings with potential clients were of closed nature and took a form of exclusive business meetings during which the purchase and sales agreement was signed. The buyer did not actually purchase pieces of art and transactions were only confirmed by a certificate.

Cash due to the above-mentioned agreements was credited to accounts maintained for the aforementioned company in a Polish bank. In total, the equivalent of about PLN 300 million was received over a period of about 10 months. The funds were subsequently transferred to various persons and entities. Their partial return to the above accounts was intended to create the impression of conducting legal transactions. The probable objective of such activities was only to pretend investing funds in advisory firms, potentially dealing with the generally accepted cultural activity.

667. Under the "cross-border transfers" method, both cash transactions linked and not linked to a payment account can be used (e.g. a cash payment combined with a cash withdrawal order to another entity in another country). Sometimes money transferred by this method outside the country, after passing through several stages of money laundering, went back to the country.

Example no. 2[316]

Funds originating from the EU grants were transferred through bank accounts maintained in various countries to companies established abroad whose shareholders were Polish citizens. Ultimately, the funds went to Poland. Some of the funds were transferred to the accounts of entities affiliated with companies receiving subsidies from EU funds, from where they were paid out in cash. Entities receiving grants from the EU may have misused them by transferring the funds received abroad to affiliated entities. These transactions deviated from actual economic events.

668. The "straw men" method consists in recruiting natural persons by criminals to set up companies, open accounts, establish powers of attorney for company accounts. Such persons, who are often in a difficult financial situation, lend their personal data for a certain fee to carry out these activities and to legitimise activities related to these companies and accounts. They usually do not affect the actions and transactions undertaken. Their potential contacts with public authorities and credit and financial institutions undertaken in connection with the operation of the above mentioned companies and accounts are closely controlled by criminals.

669. Regular actions against so-called "money mules" have been initiated in the EU since 2016. They are coordinated by Europol and Eurojust in cooperation with the European Banking Federation. The term "money mules" means a specific category of "straw men" which are - often without knowing the real purpose - recruited by criminal groups for money laundering. Encouraged by the promise of easy money, they transfer money on behalf of other people and entities between accounts often held in different countries. In the period from 2016 to May 2018, more than 2,000 "money mules" were identifies and 400 were arrested.[317] The last action of this type (under the name of *the fourth European Money Mule Action "EMMA 4"*) was carried out in the second half of 2018 with the participation of Polish law enforcement agencies as well as law enforcement agencies from 29 other countries (including 4 non-EU agencies). The action was supported by more than 300 banks, which helped - together with 20 associations and other financial institutions - to identify 26,376 suspicious transactions, preventing losses in the range of EUR 36.1 million. Over 3 months, from September to November 2018, law enforcement agencies identified 1,504 "money mules" and 140 people recruiting them; moreover they arrested 168 people. In connection with this action, 837 criminal proceedings were initiated[318]

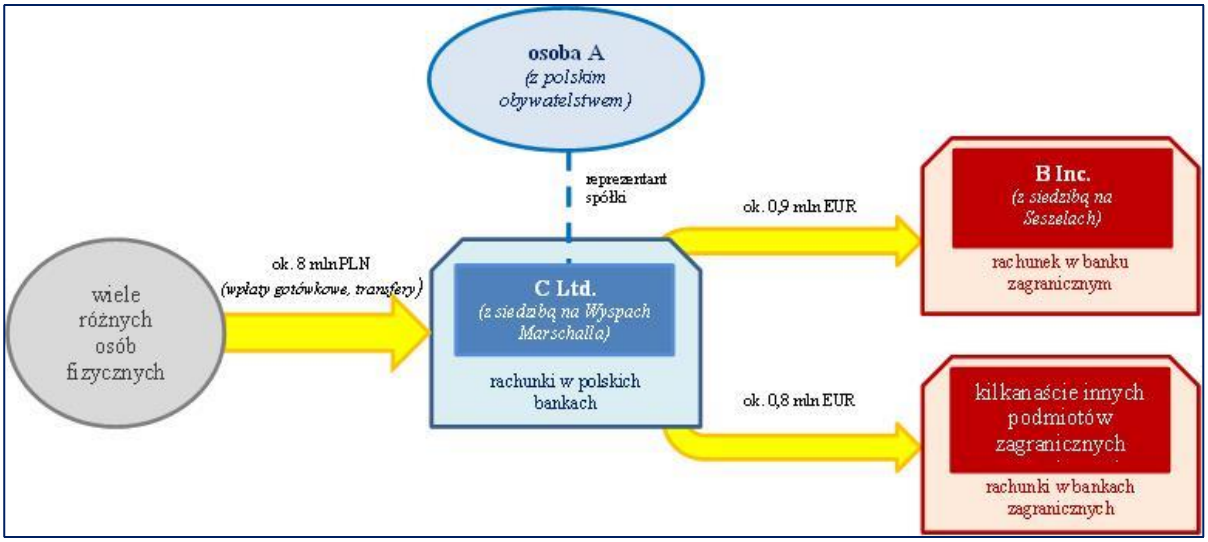
670. "Simulation companies" are usually companies or natural persons registered as sole proprietors, controlled by criminals. The purpose of their activities is to simulate conducting of legitimate business activities as a cover for transactions aimed at introducing funds from illegal activities into business transactions. Perpetrators often create complex and long chains of

[316] An example derived from *the Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2015,* p. 24.
[317] Based on information from Eurojust as of 31 May 2018. - see: http://www.eurojust.europa.eu/press/News/News/Pages/2018/2018-05-31_EMMA.aspx.
[318] Based on Europol information, see https://www.europol.europa.eu/newsroom/news/over-1500-money-mules-identified-in-worldwide-money-laundering-sting access 27 December 2018.

organisational and ownership links between such operators as well as associations, charities, trusts (with the involvement of entities registered in different jurisdictions, including tax havens) to make it difficult to identify the real owners of entities used for money laundering. The services of the so-called "virtual offices" are often used to establish and run "simulation companies". They consist in using specialised persons and companies to carry out the procedure related to the establishment of the company as well as to provide office services without the necessity of the company physical presence in the place of the declared registered office.

671. The use of the "simulation company" method can be combined with the use of services of professionals who deal with creating and running of various types of companies for the benefit of third parties - their clients. Below, the case of using a "simulation company", established in a tax haven to launder money coming from the illegal trade in illicit psychoactive substances is presented.

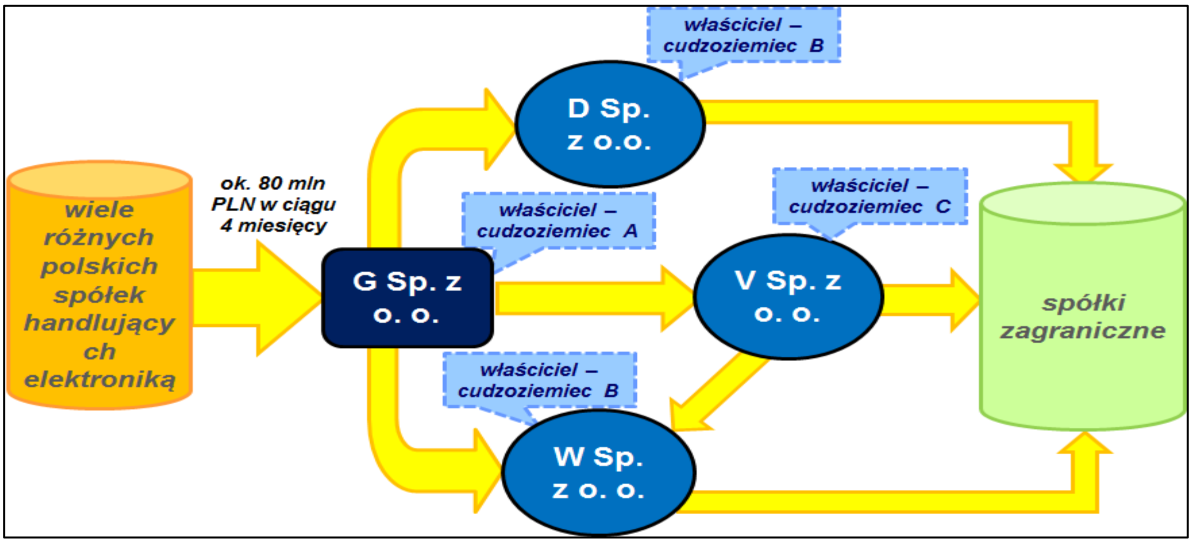
Example No. 3 - Money laundering with the use of a simulation company



Przykład nr 3	
Osoba A (z polskim obywatelstwem)	Person A (with Polish citizenship)
Reprezentant spółki	Company representative
Wiele różnych osób fizycznych	Many different natural persons
Ok. 8 mln PLN (wpłaty gotówkowe, transfery)	Approx. PLN 8 million (cash deposits, transfers)
C Ltd. (z siedzibą na Wyspach Marshalla) rachunki w polskich bankach	C sp. z o.o. (based in Marshall Islands) accounts in Polish banks
Ok. 0,9/0,8 mln EUR	Approx. EUR 0.9 million / EUR 0.8 million
B Inc. (z siedzibą na Seszelach) rachunek w banku zagranicznym	B S.A. (based in the Seychelles) account in a foreign bank
Kilkanaście innych podmiotów zagranicznych Rachunki w bankach zagranicznych	More than a dozen of other foreign entities Accounts in foreign banks

672. On the other hand, example no. 4 below shows the use of "simulation companies" (i.e. companies D, G, V and W), established in Poland, both for committing the predicate offence (in this case, a fiscal offence) and money laundering. They were established by the same person within one month in different cities, with a minimum share capital. Foreigners were indicated as owners of companies.

Example No. 4 - Laundering money coming from a VAT carousel.



Przykład nr 4	
Wiele różnych polskich spółek handlujących elektroniką	Many different Polish companies trading in electronic goods
Ok. 80 mln PLN w ciągu 4 miesięcy	Approx. PLN 80 million over 4 months
Właściciel – cudzoziemiec A/ B/ C	Owner – foreigner A / B/ C
Spółki zagraniczne	Foreign companies

673. Entities operating in financial centres or tax havens are often used for this type of activity[319] and related "simulation companies" or various types of charitable entities, also used for money laundering, are established in different countries. This is intended to make it more difficult to obtain information on the activities of these entities and detect links between them.

674. Major international scandals in recent years, such as *Offshore Leaks*, *Bahamas Leaks*, *Panama Papers or Paradise Papers*, prove that such services are often used not only by organised criminal groups but also by individuals to conceal assets (often derived from such predicate offences as corruption or fiscal crimes) from authorities of individual countries.[320]

675. The information published in connection with the above mentioned scandals by *the International Consortium of Investigative Journalists* shows that among entities involved there were also entities associated with Poland (in the case of the *Panama Papers* scandal - the above-mentioned Consortium identified 293 such entities). Verification activities were carried out at the Ministry of Finance in order to determine whether there have been infringements of tax regulations in connection with their activities. Moreover, the GIFI performed analytical investigations concerning the suspicious activities of some of these entities.

676. It is worth noting the growing number of identifications of other money laundering methods (in 2018, their share in the total number of identifications of money laundering

[319] A report published in December 2015 by Global Financial Integrity (in cooperation with some institutes and universities worldwide) indicates that the terms "tax haven", "offshore financial centre" or "secrecy jurisdiction" are often used interchangeably. There is no uniform definition for defining the phenomenon hidden behind these terms, although some characteristics of the countries they define can be identified (in particular, tax privileges for foreign investors, restrictive approach to the secrecy of commercial or banking information, procedural facilitation in setting up and running companies or trusts, poor supervision over their activities) - see: "Financial Flows and Tax Havens. Combining to Limit the Lives of Billions of People", GFI, 2015, pp. 31-35.

[320] In addition, tax havens are often used to optimise the activities of business entities in a broad sense. This is often based on the transfer of ownership of intangible rights or lending them under basic licenses at a low price to subsidiaries registered in tax havens, which accumulate the profits associated with their possession.

methods more than doubled compared to the previous year). Among them, the most frequently identified method, not directly related to products and services offered on the financial market, was the mixing of income gained from both legal and illegal activities (the so-called "blending"). Criminals often use business operators under their control (established for this purpose or already existing acquired entities) for its application.

677. Criminals usually combine various types of methods in order to separate property values from the source of their criminal origin even more effectively. To that end, they use simple methods such as the "smurfing" method, usually applied in the initial phase of money laundering (consisting of shredding cash transactions, using as many people as possible, ordering transactions below the threshold value, committing the obligated institution to register transactions), jointly with more complex methods.

678. The growing number of analytical proceedings conducted by the GIFI related to the suspicion of money laundering using, among others, virtual currencies is also worth attention.[321]

Example No. 5[322]

One of the analytical proceedings instituted in 2017 was related to the attempted execution of transfers ordered by a Polish company in favour of a foreign company for the total amount of approx. EUR 3 million. The funds originated from the account of one of exchanges dealing with virtual currency exchange. The information acquired implied that a representative of the aforementioned Polish company could have been associated with the activity of a criminal group dealing with VAT fraud.

The sole phase of depositing funds originating from crime took several years and it was quite limited, without raising major suspicions of the obligated institutions. In this phase, natural persons were used as well as limited liability companies belonging to those persons, through the accounts of which Bitcoins were purchased via intermediation of recognised virtual currency exchanges.

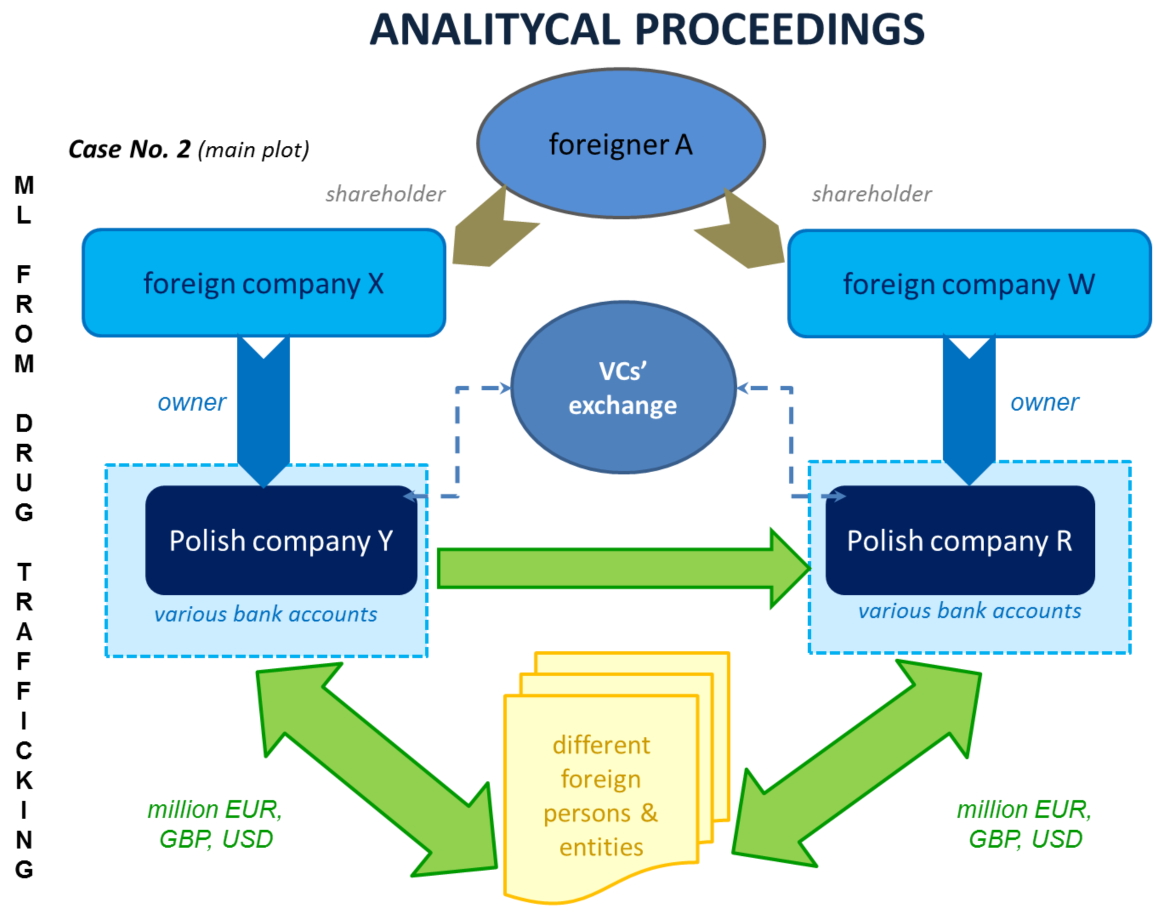
In mid-2017, the perpetrators decided to realise profits gained due to a significant increase of the Bitcoin exchange rate, establishing a new limited liability company using a substitute person and trying to transfer funds received by this economic operator abroad, to one of tax havens.

In total, the GIFI blocked 5 bank accounts where funds with the total value of approx. PLN 30.7 million were collected. It sent two main notifications and two supplementary notifications to the prosecutor's office in the above mentioned case.

[321]The definition of virtual currency is presented in Article 2(2)(26) of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing.*

[322] An example derived from *the Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2017*, p. 26.

Example No. 6 - Laundering money originating from illegal activities pursued abroad.



679. When describing the procedure of money laundering with the use of virtual currencies, it is also worth noting that the products and services offered in our country may also be used to launder money coming from illegal activities undertaken abroad. Example No. 6, based on one of the analytical proceedings conducted by the GIFI in 2018, presents the use of the Polish financial system to launder money from drug trafficking. At the same time, it is worth emphasising that illegal profits, before their transferring to Poland, were laundered through one of the foreign cryptocurrency exchanges. In this case, the GIFI suspended 4 transactions with an equivalent of approximately EUR 16.3 million and blocked accounts where cash in the total equivalent of approximately EUR 59.0 million was accumulated.

6. RISKS RELATED TO FINANCING OF TERRORISM

6.1. THREAT OF TERRORISM

680. International terrorism is one of the most serious contemporary threats to global security. Countries and regions facing problems related to respect for democracy and human rights and a free market economy are particularly exposed to terrorism. The developed countries of the West are also a place of terrorist attacks. An important factor influencing the development of terrorism are strong separatist tendencies and national, religious, social and racial divisions. The scale of the phenomenon often goes beyond the borders of individual countries or regions, becoming, like e.g. Al Qaeda and ISIS, a threat of global dimension. Due to the complexity of the problem, terrorism is becoming a permanent feature of international policy in the foreseeable perspective.

681. A terrorist offence is defined in *the Act of 6 June 1997 - Penal Code*. Article 115 § 20 of this Act indicates that an offence of a terrorist nature is a prohibited act subject to the penalty of deprivation of liberty of at least 5 years, committed with the aim to:

- seriously intimidate many people,
- force a public authority of the Republic of Poland or another country or an authority of an international organisation to undertake or abandon specific actions,
- cause serious disturbances in the system or economy of the Republic of Poland, other country or international organisation

- as well as the threat of committing such an act.

682. The key legal act for the Polish system of counteracting terrorist threats is *the Act of 10 June 2016 on counter-terrorist activities* (Journal of Laws item 904, as amended) which entered into force on 2 July 2016. The systemic approach to the issue of threats of terrorist nature applied in this regulation is intended to make it possible to use the potential of all services, bodies and institutions with statutory powers to carry out counter-terrorist activities and to positively influence the speed and accuracy of the decision-making process at the strategic level. The basic aim of the regulation is to increase the effectiveness of the Polish counter-terrorist system, and consequently to increase the security of all citizens of the Republic of Poland, through: strengthening of coordination mechanisms, clarifying the tasks and responsibilities of individual services and authorities and the rules of cooperation between them, ensuring a possibility of effective actions in the event of a suspected terrorist offence,

including in the scope of preparatory proceedings, providing for response mechanisms adequate to the type of threats involved and adjusting criminal legislation to new types of terrorist activities.

683. The Internal Security Agency plays the leading role in identifying threats related to terrorism - pursuant to *the Act of 10 June 2016 on counter-terrorist activities*, which has been reflected, inter alia, by indicating in the said Act the responsibility of the Head of the ABW in relation to the prevention of terrorist events. Pursuant to Article 5(1) of the aforementioned Act, the Head of the ABW coordinates analytical and informational activities and the exchange of information between services in the scope of events of terrorist nature. Moreover, under Article 8(1) of this Act, the Head of the ABW is also responsible for coordinating operational and exploratory activities of other services in this area. The Border Guard, the Police and other services and institutions support the activities of the ABW in this area, inter alia, within the framework of the Counter-Terrorist Centre of the Internal Security Agency (CAT ABW). The cooperation of the aforementioned services and institutions consists primarily in providing all information obtained by officers, which is included in the catalogue of incidents and events to be reported to CAT ABW, as well as conducting direct cooperation in case of recording events indicating a potential terrorist threat. On the other hand, the minister competent for internal affairs was designated as responsible for preparing to taking control over events of terrorist nature by means of planned undertakings, reacting in the event of the occurrence of such events and removing their effects, including the restoration of resources used to respond to such events.

684. The level of terrorist threat is determined on the basis of the provisions of *the Act of 10 June 2016 on counter-terrorist activities* which introduced a universally applicable system of alert degrees. Notwithstanding the foregoing, it should be pointed out that monitoring, analysis and evaluation of terrorist threats is the responsibility of the Inter-ministerial Team for Terrorist Threats[323] chaired by the Minister of Internal Affairs and Administration.

685. According to information held by the Ministry of the Internal Affairs and Administration, in the years 2012-2016, 13 persons were charged with crimes of a terrorist nature[324]

686. Many services and institutions participate in the Polish counter-terrorist protection system. Their participation in the system consists in the implementation of statutory provisions relating to the phenomenon of terrorism. The services and institutions concerned include: MSWiA, MSZ, GROM, ABW, Intelligence Agency, Military Intelligence Service, Military Counterintelligence Service, Police, State Fire Service, Border Guard, State Protection Service, GIFI, Customs and Tax Control Service, Government Security Centre, National Security Office.

687. Pursuant to *the Act of 10 June 2016 on counter-terrorist activities* , the Head of the Internal Security Agency shall keep a list of persons who may be related to terrorist events. The list includes information on, inter alia, persons engaging in activities for terrorist organisations or organisations linked to terrorist activities or members of such organisations, as well as persons participating in terrorist training or travelling in order to commit a terrorist offence. The creation

[323] The Inter-ministerial Team for Terrorist Threats was established on the basis of Regulation No. 162 of the Prime Minister of 25 October 2006.

[324] Based on the information provided in the reply of the Ministry of Internal Affairs and Administration of 6 November 2017 to the Parliamentary question No 15973, available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

of the above-mentioned database is a consequence of the increase in the occurrence of terrorist events. In the contemporary reality of the struggle against terrorism, the ability to identify quickly a person involved in a terrorist event is essential to prevent, combat and mitigate the effects of such crime. The aforementioned list also allows for the exchange of data with third country services.

688. One of the main challenges for our country related to the terrorist threat is the geographical location of Poland. Due to the fact that the Eastern border of the Republic of Poland is at the same time the border of the Schengen Area, the routes for the transportation of people and goods from the Eastern direction - countries of the former USSR and from Central and South-Eastern Asia - across our country. These routes may be used by people associated with terrorist groups (including those returning from FTF conflict zones[325]), which involves both a potential threat to Poland and to our image on the international arena. In a similar context, the existing freedom to travel within the Schengen area has an impact on the terrorist threat in our country. Many EU Member States face the problem of Islamic radicalism (e.g. Belgium, France, Germany), which means a potential opportunity for radicals to travel freely across Europe, including Poland. In the past, there have been cases where the planning and preparation of an attack took place in a country other than the location of the attack itself.

689. In Polish conditions, however, the increase in radicalism in the Muslim diaspora in Poland is alarming, both among foreigners living in our country and Polish converts. Free access to the propaganda materials of terrorist groups via the Internet as well as contacts with already radicalised followers of Islam abroad play an important role here. Experience shows that the most effective method of counteracting extremist-terrorist threats is to respond early to the first symptoms of radicalism in the society. Only a properly designed and well-functioning system of preventive measures affecting individuals and population groups that are susceptible to extremist ideologies can ensure the achievement of this objective. One of the system activities is the creation of the ABW Terrorist Prevention Centre (ABW CPT) within the ABW structure. The Centre specialises in the broadly understood prevention of terrorism, the key element of which is to disseminate knowledge about the possibilities of preventing events adverse from the security perspective. In this respect, the ABW CPT[326] provides tailor-made training courses for officials and staff of special services as well as for public administration bodies and other entities. The aim of the Centre is to create a broader prevention mechanism based on cooperation of all public administration entities and citizens in the process of shaping a culture of security in Poland. The Centre aims to bring together the knowledge and experience of special services, public institutions as well as the achievements of universities and scientific institutions, becoming a forum for the development of cooperation between all entities of the security system.

690. If there is a justified suspicion that foreigners (including citizens of EU Member States and their family members) carry out terrorist or spying activities, or those foreigners are suspected of committing one of those offences, the decision on obliging to return or expulsion is taken by the minister competent for internal affairs at the request of the Commander-in-Chief of the Police, the Head of the ABW or the Head of Military Counterintelligence Service. Entrusting the competence in this respect to the minister competent for internal affairs is justified due to

[325] Abbreviation for *foreign terrorist fighters*.
[326] https://tpcoe.gov.pl/cpt/o-nas , date of reading 2 May 2019

the special importance of the state's activities in the field of counteracting terrorism (in other cases provided for by law, the governor of the province, the commander of the SG troop or the commander of the SG facility remain competent to take the aforementioned decision). Bearing in mind the potential significant threats to the state security posed by a person expelled under the above procedure, it is envisaged that the decision of the minister competent for internal affairs will be subject to immediate, compulsory execution. The Prime Minister, as a higher authority, will have the right to appeal against this decision[327]

691. Poland is inhabited by representatives of 9 national minorities (Belarusians, Czechs, Lithuanians, Germans, Armenians, Russians, Slovaks, Ukrainians, Jews) and representatives of 4 ethnic minorities (Karaims, Lemkos, Roma, Tartars)[328] Moreover, Kashubians, a community using the regional language, live on the territory of the Pomorskie Province. Germans represent the largest national minority. During the National Census of Population and Housing conducted in 2011, German nationality was declared by 144,238 Polish citizens (according to the data of the previous national census of 2002, the German minority comprised 147,094 people).

692. In order to protect the Eastern and Northern border of Poland (which is also the Schengen area border) against illegal inflow of immigrants, the state border of the Republic of Poland is constantly monitored by foot patrols and using vehicles (passenger, off-road, motorcycles, quads, and in winter also snowmobiles) and aircraft available in the equipment of the Border Guard (including drones). At sections where the national border runs along watercourses or water reservoirs, vessels are used for service. Additionally, for the protection of the state border, among others, observation towers equipped with long-range thermal imaging cameras, observation vehicles, portable thermal imaging cameras, portable perimeter sets, night vision goggles and modern binoculars are used. In addition, an arable belt is maintained at certain sections of the national border, where the terrain allows, to quickly identify illegal border crossings and determine the number of illegal migrants and their possible direction of movement[329]

693. Activities in the scope of provision and exchange of information between the SG and the border services of the neighbouring countries are carried out on an on-going basis. These activities consist in a daily, mutual exchange of statistical data and the provision of any information that may affect the protection of the national border or the flow of the border traffic.

694. The border of the Republic of Poland is protected along its entire length, with particular emphasis on the sea, air and land sections of the border with the Russian Federation, the Republic of Belarus and Ukraine, which constitute the external border of the EU and the Schengen area. Contrary to the meaning of absolute numbers, the Border Guard considers the section of the border with Lithuania, where the statistics are significantly lower, but which represents an intensive stream of illegal immigrants from third countries towards the interior of

---

[327] On the basis of the reply of the Ministry of Internal Affairs and Administration of 2 August 2016 to the Parliamentary question no. 3999 (on the threat of terrorist attacks on Poland and actions taken at the country borders to ensure internal security and the infiltration of people who may pose threat to the security of Poles), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

[328] http://mniejszosci.narodowe.mswia.gov.pl/mne/mniejszosci/charakterystyka-mniejs/6480,Charakterystyka-mniejszosci-narodowych-i-etnicznych-w-Polsce.html, date of reading 10 May 2019.

[329] On the basis of the reply of the Ministry of Internal Affairs and Administration of 2 August 2016 to the Parliamentary question no. 3999 (on the threat of terrorist attacks on Poland and actions taken at the country borders to ensure internal security and the infiltration of people who may pose threat to the security of Poles), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

the EU, which is mostly handled by organised criminal groups, as the most threatened section of the internal border.[330]

695. Within the framework of the implementation of the "National Counter-Terrorism Programme for the years 2015-2019", the implementation of which is the responsibility of the Minister of the Internal Affairs and Administration, measures were and are taken in order to strengthen the migration recognition in relation to foreigners coming from high-risk countries, staying on the territory of the Republic of Poland, potentially exposed to the phenomenon of radicalisation and recruitment to terrorist organisations. There are also activities aimed at strengthening the tools enabling current monitoring of the inflow of foreigners to the Republic of Poland, especially from high-risk countries and regions and countries subject to conflicts, in order to determine in advance the phenomena of mass migration. Within the framework of the above mentioned activities, guidelines were issued, inter alia, on intensifying operational investigation in relation to foreigners entering and staying on the territory of the Republic of Poland and leaving this territory who come from countries of higher risk as well as regions and countries subject to conflicts, in terms of belonging to terrorist organisations, and the concept of "Monitoring of entry and stay of foreigners on the territory of the Republic of Poland in terms of identifying threats to the state security and public order" was implemented (the document is classified)[331].

696. In the framework of counteracting terrorism by EU border services, risk indicators have been developed in cooperation with the European Border and Coast Guard Agency (Frontex) and Europol for the control of the so-called "Foreign Terrorist Fighters” on external borders[332]. The said indicators shall, on the basis of the information available, constitute a list of criteria for the identification of these persons during border control.[333]

697. According to the data derived from the report of the Institute of European Affairs Foundation entitled "Immigration from OIC countries to Poland in 2013-2018" (the survey concerned citizens of countries of the Organisation of Islamic Cooperation - OIC[334] which associates countries with a Muslim majority) between 2013 and 2018, the number of foreigners from OIC countries holding a residence permit in Poland increased almost threefold, mainly due to the dynamically growing number of people staying on the basis of a temporary stay. In mid-2018, the number of foreigners from Muslim countries residing in Poland legally amounted to 20,910 people, of which almost 75% stayed on the basis of the temporary residence permits (and taking into account pending applications - about 27 thousand people). Dynamic growth started in 2014 and intensified in the following years[335].

---

[330] On the basis of the reply of the MSWiA of 6 November 2017 to the Parliamentary question No. 15973 (concerning the terrorist threat in Poland), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

[331] On the basis of the reply of the MSWiA of 27 January 2017 to the Parliamentary question No. 8777 (concerning centres for refugees on the territory of the Republic of Poland), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

[332] FRONTEX - Introduction of Common Risk Indicators, January 2018. (limited dissemination).

[333] On the basis of the reply of the MSWiA of 4 December 2017 to the Parliamentary question No. 16902 (concerning ISIS members returning to our country), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

[334] Abbreviation for *Organisation of Islamic Cooperation.*

[335] Jan Wójcik, Immigration from OIC countries to Poland in 2013-2018, ed. Institute for European Affairs Foundation, pp. 4-6, available at: http://europeanissues.org/wp-content/uploads/2018/11/Imigracja-do-Polski-z-OIC-lata-2013-18.pdf.

698. Before a foreigner enters the SG officers perform a number of activities aimed at verifying, apart from establishing the identity of the foreigner and his/her entitlement to enter or stay on the territory of the Republic of Poland, the compliance of the actual purpose of entry or stay on the territory of the Republic of Poland with the declared purpose. The SG officers carry out checks in domestic and foreign IT systems in order to verify the documents and explanations presented by the foreigner and to determine whether Poland or other countries have not introduced any objections towards the foreigner related to the threat to public security and order. Depending on the type of IT system and the circumstances of the case, checks may be carried out on the basis of alphanumeric or biometric data. Depending on the outcome of the checks and the situation in which the check is carried out, SC officers shall be entitled to take the appropriate measures, including a decision to refuse entry, to issue a decision committing to return, as well as to arrest and transfer to the competent authority for further action. The SG officers shall carry out an ongoing analysis of information obtained in the course of their border service concerning threats of terrorist acts[336]

699. Entities and special services participating in the Polish counter-terrorist system are obliged to provide the Counter-Terrorist Centre of the Internal Security Agency with any information available on terrorist incidents specified in the *Ordinance of the Minister of Internal Affairs and Administration of 22 July 2016 on the catalogue of terrorist incidents* (Journal of Laws of 2017 item 1517 as amended). The regulation in question, among individual categories of incidents subject to classification, includes, among others, "departure or planning of departure of a person or persons from the territory of the Republic of Poland to the area of armed conflict taking place with the participation of organisations of terrorist nature or return from that area". This applies primarily to so-called "Foreign Fighters", including those coming from EU Member States.

700. According to data contained in the EU Terrorism Situation & Trend Report (Te-Sat 2018), throughout 2017 Poland did not report any departures or returns of Polish FTFs, however, the Chechen FTF with refugee status in Poland was detained in 2017 and accused of participation in a foreign military organisation and illegal possession of weapons and ammunition.[337]

701. The Police cooperate with CAT ABW on a permanent basis with regard to the exchange of information, in accordance with the catalogue of terrorist incidents specified in *the Ordinance of the Minister of Internal Affairs and Administration of 22 July 2016 on the catalogue of terrorist incidents*. On an ongoing basis, activities carried out in individual field boards of the Central Police Investigation Bureau are also coordinated in relation to incidents involving the use of explosives on the territory of the country. The police verify all information that may indicate potential threats from terrorist organisations. The activities carried out include, among others, analysis of the occurrence of terrorist events and preparation for effective response to such an event. Officers of the "BOA" Central Counter Terrorist Subdepartment of the Police (previously Bureaux of Counter-Terrorist Operations of the Police Headquarters) successively conduct training courses and exercises at the national and international level, preparing for optimal counter-terrorist activities. The "BOA" Central

[336] On the basis of the reply of the MSWiA of 2 February 2017 to the Parliamentary question No. 8969 (concerning the internal security Poland), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.
[337] EU Terrorism Situation & Trend Report 2018, Europol, 2018, p. 26, available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018.

Counter Terrorist Sub department of the Police is a part of the EU Task Force ATLAS, which associates special intervention and counter-terrorist units in Europe. Within the framework of the above mentioned group, cooperation is carried out on an ongoing basis in the scope of exchange of experience, analysis of threats and events that have occurred. This cooperation allows to increase the capacity of the Police counter-terrorist units to neutralise terrorist threats.[338]

702. According to the available data, the threat to the security of the Republic of Poland related to religiously motivated terrorist activity remains at a low level. Poland is not in centre of the operational interest of terrorist groups and the threat of activity of people motivated by radical ideology remains low. However, in the context of terrorist incidents and attacks regularly recorded in Europe, information on FTF departures and returns, the propaganda and logistics activities of terrorist groups and factors that may contribute to the radicalisation or exacerbation of the Polish Muslim diaspora is monitored.

703. A significant threat to the threat of terrorism in the country is the phenomenon of radicalisation of the representatives of the Muslim diaspora in the Republic of Poland, which applies both to foreigners living in our country and to citizens of the Republic of Poland who converted to Islam. These people are becoming more and more radical on the basis of terrorist groups' propaganda material disseminated on the Internet as well as through contacts with radical Islam followers abroad (including the use of encrypted communicators). In extreme cases, as has happened several times in Europe recently, these people may decide to engage in armed *jihad* as so-called *lone actors*. Moreover, an increase in religious radicalisation of the Chechen diaspora staying in the Republic of Poland has been recorded. Contacts of members of this diaspora in Poland with compatriots involved in the armed *jihad* in the Syrian conflict zone and in Chechnya itself contribute to radicalisation of their attitude. Young members of the diaspora treat Chechen fighters in Syria as role models, both in terms of their religious attitude and combat skills. Therefore, combat sports clubs are increasingly becoming centres of radicalisation, associating representatives of this diaspora. More and more often, the former authorities of Chechens fighting for the country's freedom are replaced by *jihad* fighters.

704. Poland is also not completely free from the threats originating from the phenomenon of the so-called foreign fighters. According to the information available to us, about 20 people directly related to our country went to Syria in recent years, where some of them undertook active military measures on the part of Islamic terrorist groups. Another few dozen people - foreigners (mainly of Chechen nationality) should be added to this group who travelled to Syria with a legalised residence status in Poland, although they lived in other European countries. These people can gradually return to Europe, including our country.

705. On 31 August 2018, at the request of the Head of the ABW, a Chechen refugee was expelled from Poland. The request for expulsion drawn up by the Head of the ABW was formulated on the basis of the ABW's own information as well as data provided to the Polish side by the special services of partner countries and international entities. The reason for the expulsion was information that the above-mentioned person left Belgium for the Middle East in 2014 and fought in the ranks of ISIS. On his return to Belgium, he maintained contacts with

[338] On the basis of the reply of the MSWiA of 12 July 2017 to the Parliamentary question No. 13252 (concerning the security of Poland in connection with the terrorist attack in the United Kingdom), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

the radical community, as well as with those involved in arms smuggling. According to the information provided to ABW by the partner services, the person was treated by the German services as a member of a terrorist organisation, he was also mentioned as a person involved in human smuggling and money laundering. In 2017, Europol entered him in the list of supporters of terrorist organisations and also qualified him as an Islamic fighter. Due to his links with terrorist organisations, the aforementioned person, staying in Belgium, was detained by the Belgian authorities and expelled from the country in March 2017. He has also received a 10-year ban on entry into Belgium. Due to the fact that the aforementioned person had subsidiary protection granted by the Polish authorities, Belgium expelled him to Poland. In this situation, the authorities of the Republic of Poland had no other option but to oblige the above-mentioned person to leave the territory of our country. At the same time, it is known that the above-mentioned person had travelled to Russia in 2009, from where he returned to Belgium. He reported his departure during the proceedings conducted by the Belgian Immigration Office. The above mentioned person informed that in 2009 he had arrived in Chechnya and then stayed in Ingushetia, from where he returned to Belgium with his wife and two children (in September 2009). He stayed officially in the Russian Federation, and faced no repressions at that time. This fact was taken into account when formulating the application for expulsion of the above-mentioned person from Poland. The decision in this case was taken by the Minister of Internal Affairs and Administration at the request of the Head of the ABW. The above mentioned person was expelled and also received a five-year ban on entering the territory of the Republic of Poland and other Schengen countries.[339]

706. Currently, one of the most important factors influencing the level of terrorist threat in Europe is the widespread access to terrorist groups' propaganda material on the Internet, which has a significant impact on the increase in *homegrown terrorism* - cases of radicalisation leading to terrorist attacks. Such materials are also commented on and distributed by Polish network users.

707. In addition to religiously motivated terrorism, potential threats can also be generated by groups that refer to extreme political ideologies - both right-wing and left-wing. According to the information available, Polish extremist groups do not currently generate direct threats to the state internal security. Their activity consists mainly in organising manifestations, celebrations of historical anniversaries, concerts, fighting tournaments and other actions related to the promotion of extreme ideologies. Only occasionally representatives of these circles undertake actions of a hooligan or criminal nature, inspired by their ideology. The activities of right-wing and left-wing groups are also monitored in the context of hybrid threats and possible inspiration of certain groups by persons linked to foreign special services (including the organisation of terrorist acts).

708. In the EU Terrorism Situation & Trend Report (Te-Sat 2018), Europol stated that European *right-wing extremist* groups (RWE) have extensive international contacts. For example, the Belgian RWE groups have established contacts with similar groups in Bulgaria, Germany, Poland, Russia, USA and Austria. In the Polish context, this report also states that during the demonstration in Slovakia against the influx of immigrants, which was also attended by non-

---

[339] Response of the Minister - member of the Council of Ministers, coordinator of special services of 11 October 2018 to the question of the MP of the Republic of Poland No. 7953 (concerning the expulsion of the Chechen refugee from Poland), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

extremist right-wing participants, delegates from Belgium, the Czech Republic, Germany, Hungary and Poland took part (source - EU Terrorism Situation & Trend Report (Te-Sat 2018).[340]

709. On 21-22 April 2018, ABW officers, supported by the Police, carried out activities in Dzierżoniów (Dolnośląskie Province). A neo-Nazi concert was then thwarted. Materials used to promote the Nazi system were found on the spot: banners and flags and other items referring to the Nazi symbols. Two organisers of the concert were detained. Both suspects have been in the focus of the ABW interest for many years and have been active in neo-Nazi circles since the 1990s. They were one of the most important people of this stream in Poland. The men had international contacts with, among others, neo-Nazis from Serbia, the Czech Republic, Ukraine, France and Great Britain. They had particularly close relations with neo-Nazis from Germany, including the leaders of the local *Blood & Honour* cells. The concerts organised several times a year by suspects were attended by 100 to even 500 participants. Ticket prices for such performances ranged from PLN 100 to PLN 120. With an average number of 300 participants, this gives a revenue of PLN 30 thousand. The funds obtained in this way constituted a source of financing for local neo-Nazis. The additional income was generated from the sale of alcohol, foodstuffs as well as records and T-shirts which contain Nazi symbols and content. The detained men were the leaders of the Lower Silesian informal organisation Blood & Honour. The Group operated under the name "Club 28" (Numbers 2 and 8 correspond to letters of alphabet: B for "blood" and H for "honour"). The peak of the suspects' activities was 2017 when as many as four neo-Nazi concerts were organised. One of them was the "Ironborn Relise Party" - an event moved from the Czech Republic since the local services did not admit its organisation. The Regional Prosecutor's Office in Walbrzych presented both men with charges concerning the organisation of five neo-Nazi concerts between March 2016 and April 2018, during which the content of a totalitarian - fascist nature was promoted, hatred was incited against national, ethnic and racial differences, as well as content of a fascist symbolism was presented[341]

710. The Internal Security Agency fulfils its statutory obligations on an ongoing basis. Tasks of the Internal Security Agency are laid down in Article 5 of the *Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency* (Journal of Laws of 2018, item 2387 as amended). They include "identifying, preventing and combating threats to the internal security of the State and its constitutional order, in particular its sovereignty and international standing, independence and integrity of its territory as well as the defence of the State". As part of its activities, ABW monitors radical environments. Due to the nature of activity of radical organisations, the ABW conducts both operational and analytical activities in this area. While fulfilling its statutory obligations, the Agency provides the most important persons in the country with reports and studies on the issue of extremist threats in Poland[342]

[340] EU Terrorism Situation & Trend Report 2018, Europol, 2018, pp. 51-52, available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018
[341] Spokesman of the Minister Coordinator of Services - PAP Press Centre, 30 April 2018, http://centrumprasowe.pap.pl/cp/pl/news/info/119156,36,akcja-abw-w-dierzoniowie-dodatkowe-informacje-(communication), date of reading: 2 May 2019
[342] The reply of the Minister - Coordinator of the Special Services of 28 February 2018 to the Parliamentary question No. 19011 (concerning the information on extremist threats provided to the President of the Republic of Poland and the Prime Minister by special services), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.

711. False notifications of putting the explosives, due to their social harmfulness, disorganisation of the functioning of the notified entities (including public institutions and public utility facilities), constitute a potential threat to life and health of people evacuated e.g. in hospitals). On the other hand, the resulting financial outlays incurred make an important problem from the national perspective. The disinformation nature of false notifications of the deployment of explosives has the potential to be used by terrorist organisations in their tactics to carry out real-life attacks and to test the readiness and modus operandi of relevant services.

712. In terms of identifying and combating threats of a terrorist nature and the criminal terror, in 2018 the Central Bureau of Investigation of the Police recorded 11 explosions (in 2017 -20), caused by the use of explosives, pyrotechnic mixtures and flammable substances (with a system having the characteristics of an explosive device), including 3 cases with the characteristics of criminal acts of terror (in 2017 - 8). In 2018, The CBŚP revealed 11 cases of placing explosive devices (in 2017 there were also 11 similar cases). In eight cases, the devices were neutralised by the miners-pyrotechnicians while in three cases the explosive devices exploded. 6 dummies of explosive devices were also revealed (in 2017 - 7). In 2018, the CBŚP recorded 218 false notifications of placing an explosive charge (in 2017 - 260), which covered 286 different types of public institutions and state facilities as well as other entities (in 2017 - 643). The highest intensity of false notifications was recorded in the Mazowieckie Province, i.e. 75 (in 2017 - 80). As a result of actions taken by the CBŚP, 104 perpetrators of false notifications were detained (in 2017 - 102). The detection rate of this type of crime in 2018 was 52% (in 2017 - 39%). Cascade alarms represented a special form of reporting. They relate to the communication by one perpetrator of a threat to more than one facility at the same time or at a similar time using the same means of communication. It has been assumed that a report of simultaneous threat for at least two facilities should be considered a cascade alarm. In 2018, 4 cascade notifications were recorded (2017 - 6), covering more than half of all facilities exposed to this procedure. In the area of combating organised crime, CBŚP officers in 2018 dealt, inter alia, with the combating of organised groups involved in the illegal production and trafficking of weapons and ammunition, theft of luxury cars and kidnapping for ransom. In 2018, the CBŚP secured the total of 391 firearm pieces (in 2017 - 363), including: short weapons - 169 (in 2017 - 143), long weapons - 86 (in 2017 - 73), gas weapons - 110 (in 2017 - 17) and other, i.e. machine guns, signal guns, alarm guns, self-propelled guns, gunshells - 26 (in 2017 - 130)[343]

713. The Counter-Terrorist Centre of the Internal Security Agency operates within the ABW structure. The Centre is a coordination and analytical unit for preventing and combating terrorism. The CAT operates on a 24/7 basis. Apart from ABW officers, the service is provided by delegated officers, soldiers and employees of, among others, the Police, the Border Guard, the Government Protection Bureau, the Intelligence Agency, the Military Intelligence Service, the Military Counter-intelligence Service and the KAS. They implement their tasks within the competence of the institution which they represent. Moreover, other entities participating in the system of counter-terrorist protection of the Republic of Poland actively cooperate with the Counter-Terrorist Centre, such as the Government Security Centre, the Ministry of Foreign Affairs, the State Fire Service, the GIFI, the General Staff of the Polish Army, the Military Police, etc. The essence of the CAT ABW system functioning is to coordinate the process of

[343] Report on the activities of the Central Bureau of Investigation of the Police for 2018 (in statistical terms), Warsaw 2018, available at: http://www.cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

information exchange between the participants of the counter-terrorist protection system, enabling the implementation of common procedures for responding in the event of one of four categories of a defined threat: a terrorist event occurring outside Poland affecting the security of the Republic of Poland and its citizens; a terrorist event occurring on the territory of Poland affecting the security of the Republic of Poland and its citizens; obtaining information on potential threats that may occur on the territory of Poland and outside Poland; obtaining information on money laundering or transfers of financial resources that may be indicative of financing terrorist activities[344]

714. Due to the cross-border dimension of crime and terrorism as well as in connection with the abolition of border controls between Schengen States, international cooperation in preventing and combating threats to internal security has been significantly strengthened. One of its main elements is the international exchange of information between competent authorities which makes it possible to identify persons posing risk. Services subordinated and supervised by the Minister of Internal Affairs and Administration are constantly developing international cooperation, using available mechanisms such as the Schengen II Information System (SIS II), the European Police Office (Europol) or the Prüm Decisions.

715. The Internal Security Agency, fulfilling its statutory duties, identified a Polish citizen David Ł. as a person involved in planning a terrorist attack. In connection with the findings of ABW, the above-mentioned person was detained on 12 February 2019 in the area of Radom. The searches of the places where he was staying revealed a series of evidence that indicates that he had been gathering information and raising funds that he intended to use for criminal activities of a terrorist nature. The prosecutor presented the detainee with a charge of preparation for committing a terrorist offence. The court applied a preventive measure against the suspect in the form of provisional detention for a period of 3 months. The investigation in this case is carried out by the Local Department of the Internal Security Agency in Łódź under the supervision of the local National Prosecutor's Office[345] At the same time, press sources[346] report that while staying in Syria Dawid Ł. joined the Muslim Movement Dawn of Syria (Arab. *Harakat Fajr Sham al-Islamijja*) whose aim was to overthrow the political system of the regime of the Arab Republic of Syria ruled by Bashar al-Assad. It is a little known and not very significant group, entered in the list of organisations observed by the international services. It was established in 2014, i.e. at the same time when the above-mentioned person left for Syria. The Muslim Movement Dawn of Syria derives from the organisation *Dzabhat Ansar ad-Din*, which was also founded in July 2014 and is a coalition of several *Jihad* groups. It was affiliated with *Dzabhat an-Nusra*, an organisation that collaborated with al-Qaeda. David L. was first detained on charges of participation in a terrorist organisation in November 2015 at the Oslo airport, where he had arrived from Turkey. Soon - as part of the extradition - he was handed over to the Polish party. The findings of the services inform that this person returned to Europe from Aleppo. There, "to a certain extent" - according to the prosecutor's office - he took part in the combat activities of the "Muslim Movement Dawn of Syria". He also allegedly participated

344 http://www.antyterroryzm.gov.pl/CAT/antyterroryzm/instytucje-i-sluzby/agencja-bezpieczenstwa/547,Agencja-Bezpieczenstwa-Wewnetrznego.html, date of reading 2 May 2019
345 Spokesman of the Minister - Coordinator of Special Services - PAP Press Centre, 4 March 2019, available at: http://centrumprasowe.pap.pl/cp/en/news/info/135758,,rzecznik-ministra-koordynatora-sluzb-specjalnych-nt-dzialan-abw-(komunikat), decisionate of reading 2 May 2019
346 including: http://lodz.wyborcza.pl/ or https://wiadomosci.radiozet.pl of 4 March 2019, date of reading 2 May 2019

in patrols in *Jihad* occupied areas. The above mentioned person had documents which allowed him to move freely around the areas occupied by terrorist organisations at that time. David L. heard the charges and was taken into custody. His trial began after two years - in November 2017 - before the Regional Court in Łódź. However, the court decided to release the above mentioned person from custody pending trial.

716. In terms of internal security, the links between the illegal immigration and organised crime and terrorism are particularly dangerous. Migration processes can be linked to the phenomenon of terrorism through the use by terrorists of so-called 'stormtroopers' strategies or dormant cells. The strategy of stormtroopers assumes penetration into the territory of a state in order to launch a terrorist attack, previously planned on the territory of another state. The strategy of dormant cells, on the other hand, is based on the use of so-called dormant cells, i.e. groups already present on the territory of the target country which are activated at the right time to carry out a terrorist attack. In this case, we usually deal with so-called domestic terrorism. Regardless of the use of both strategies, terrorist attacks by single individuals, so-called lone wolves, inspired by the generation of a rise in radical sentiment, are carried out more and more frequently.

717. Illegal migration has for years remained the most serious form of border crime, especially in organised forms. Its combating is a priority for the Border Guard. Illegal migration is an ever-increasing phenomenon, with possible changes in the forms and methods of organisation and sources of migration flows dependent on geopolitical changes and emerging global armed conflicts or economic and humanitarian crises. Poland is treated by illegal migrants primarily as a transit country on the migration route to other countries of Western Europe and North America but for a relatively small part it is also the country of destination of migration, which is facilitated by, among others, Poland's excellent geographical location at the crossroads of Europe's main communication routes; our country membership in the Schengen area, and thus a smooth transition to Western European countries, better economic and social prospects, an attractive labour market, better wages and social and living conditions, political, religious and moral freedom.

718. In 2018, the Border Guard officers carried out a number of projects, resulting in the dismantling of organised criminal groups, including those of an international nature operating in many countries, carrying out cross-border illegal transfers of foreigners. In connection with the participation in an organised group or in a relationship aimed at committing a crime, the Border Guard initiated 46 preparatory proceedings (in 2017 - 59). The allegation of committing a crime was presented to 331 suspects (in 2017 - 352), including 88 foreigners (in 2017 - 100), among which Ukrainian citizens were predominant - 51 (in 2017 - 68). On the other hand, in the area of crossing the border, contrary to the provisions of law (i.e. Article 264§ 2 of the kk, Article 264§3 of the kk) in 2018, the Border Guard initiated 987 preparatory proceedings (in 2017 - 1 107, which indicates a decrease by 10.8%). The allegation of committing a crime was presented to 1,363 suspects (in 2017 - 1,336, which indicates an increase by 2%), including 1,188 foreigners (in 2017 - 1,158, which indicates an increase by 2.6%), with the predominance of Ukrainian citizens - 520 (in 2017 - 686).

719. Illegal migration takes place mainly with the involvement of organised criminal groups which organise transport for persons transferred at all stages of the journey, temporary shelter in the transit countries, and provide forged or falsified documents. For these organised crime groups, the profits from smuggling of people across borders are used to conduct criminal activities in other areas. These organised crime groups are extremely creative and adapt their

activities quickly to changing legal and practical circumstances. There is no single typical modus operandi in this field. The methods of illegal migration include using the so-called green border, crossing the state border of the Republic of Poland on the basis of counterfeit or forged documents authorising to cross the border, processing of border control stamps in order to confirm the "legality" of periods of stay on the territory of the EU and obtaining another visa, using the so-called *look a like* method, with the use of documents (especially Polish) belonging to other people. Quasi-legal methods are also used, which include: abuse of the possibility to enter the territory of the Republic of Poland on the pretext of taking up education, work, for tourist, business, cultural purposes, by using for this purpose false or misleading documents authorising to obtain the relevant visa; abuse of the procedure for granting the refugee status in the Republic of Poland or marriages of convenience of foreigners to Polish citizens .

720. The main identified routes for smuggling illegal migrants by land are:

- Russia - Estonia - Latvia - Lithuania - Poland - other Western European countries (the so-called Baltic route);
- Russia - Ukraine/Belarus - Poland - Germany - other Western European countries;
- Syria and Iraq - Turkey - Greece - Macedonia - Serbia - Croatia - Hungary - Austria - Slovakia - Czech Republic - Poland and further to Germany, Sweden or Finland (the so-called Balkan route).

721. In addition, air routes with different connection configurations are used on a large scale and with variable intensity. Foreigners arriving in Poland or another Schengen Agreement country try to cross the border on the basis of fraudulent Polish visas, counterfeit documents (Polish and EU) as well as documents belonging to other persons. Since illegal migration is an undocumented phenomenon, it is difficult, if not impossible, to estimate the scale of illegal immigration. Illegal migration is not subject to a single measurable criterion, there is no single formal definition of it, with a simultaneous discrepancy between the data collected in relation to illegal immigrants. Considering the foregoing, the scale of illegal migration in Poland is estimated between several dozen and several hundred thousand people. Such a large discrepancy in the estimation of this phenomenon indicates difficulties in determining the real number of foreigners with an unregulated legal status in Poland. However, taking into account a number of factors and data, such as the extent of legal migration, the number of detected illegal border crossings, estimates of illegal stay of some well-documented and recognised migrant communities, as well as the size of the residence abolitions carried out, it seems that the number of the lower range of this estimate is more likely.

722. According to the information available, in 2018, 35,990 foreigners were subject to control of the legality of their stay in Poland and 66,381 foreigners were subject to control of the legality of their employment. As a result of the controls performed, 11,388 illegally staying foreigners and 12,088 foreigners performing work without required permits were revealed (own information).

723. The development of terrorism is facilitated by a relatively new phenomenon related to the formation of so-called "parallel societies". This phenomenon mainly affects immigrant communities - immigrants not fail to integrate with the societies of the host countries, but over time, they build barriers and differences, highlighting their own distinctiveness and the lack of possibility of lasting understanding. The resulting social enclaves become "states in the state",

governed by their own laws. In such communities, not only legal immigrants function but also foreigners without a residence permit who can easily hide in groups that, in fact, are not subject to control of the legality of their residence. There is a close link between terrorist activity and human smuggling. An investigation into the attacks in Madrid in 2004 revealed that the al-Qaeda-linked group *Ansar al-Islam*, involved in the attack, dealt with the smuggling of people and counterfeiting of documents, thus financing terrorist activities and transferring its members to Spain.

724. Cooperation between institutions directly responsible for the country's internal security - including the Internal Security Agency - allows for quick and efficient identification and elimination of threats related to terrorism. The actions taken quickly enough, especially with regard to a foreigner who is afraid that he/she may carry out terrorist or spying activities or is suspected of committing one of these crimes led, inter alia, to the withdrawal of the granted subsidiary protection in 2018 and then to the implementation of actions aimed at the effective return of a citizen of the Russian Federation of Chechen nationality to the country of origin. Since the date of entry into force of *the Act of 10 June 2016 on counter-terrorist activities* until the end of 2018, the Minister of Internal Affairs and Administration issued 14 administrative decisions concerning the obligation of foreigners to return (third-country nationals) under Article 329a of *the Act of 12 December 2013 on foreigners* (Journal of Laws of 2018 item 2094 as amended) and expulsion from the territory of the Republic of Poland of EU citizens or their family members who are not EU citizens pursuant to Article 73c of *the Act of 14 July 2006 on the entry into, residence in and exit from the territory of the Republic of Poland of citizens of the Member States of the European Union and their family members* (Journal of Laws of 2019 item 293). Decisions issued in these modes relate to persons who are suspected of being involved in terrorist or spying activities or who are suspected of having committed one of these offences. The proceedings are initiated on request of: Chief Commander of the Police, Head of the ABW or Head of the Military Counter-intelligence Service. Most decisions were issued against citizens of the Russian Federation. Six decisions were issued in 2018, all at the request of the Head of the ABW.

725. The state security in the context of illegal migration is particularly visible in the case of foreigners who were detained and expelled from the territory of the Republic of Poland since it was required by reasons of defence or security of the state or the protection of public safety and order or the interests of the Republic of Poland. In 2018, 334 foreigners received decisions committing a foreigner to return due to the above mentioned circumstances, including 237 citizens of Ukraine, 72 citizens of Belarus, 8 citizens of Russia and 5 citizens of Georgia.

6.2. THREAT OF FINANCING OF TERRORISM

726. The financing of terrorism in the Polish legal system was penalised by amending the provisions of *the Penal Code*, to which the provision of Article 165a has been added. In the justification for the addition of this provision, it was indicated that: “The requirement to penalise financing of terrorism is provided for in the International Convention for the Suppression of the Financing of Terrorism, ratified by the Republic of Poland (Journal of Laws of 2004 No. 263, item 2620). Directive 2005/60/EC also applies to financing of terrorism. In

this respect, the above-mentioned regulation aims not only at full implementation of the Directive, but also at harmonising the application of international standards"[347].

727. As Professor Alicja Grześkowiak states in her commentary to the *Penal Code*,[348] the offence specified in Article 165a of the PC should be regarded as an offence in the foreground of the relevant terrorist offence which constitutes a stage of preparation for this type of act. The criminalisation of such behaviour is intended to ensure the prevention of terrorism at the earliest possible stage. The good protected by this provision is universal security and the crime itself is of universal nature. According to Professor Alicja Grześkowiak, the legislator provided for three different types of offences under Article 165a of the kk. Criminal conduct criminalised under the provision of Article 165a§1 of the kk consists in collecting, transferring or offering means of payment, financial instruments, securities, property rights or other movable property or real estate for the purpose of financing an offence of a terrorist nature or an offence referred to in Articles 120-121, 136, 166-167, 171, 252, 255a or Article 259a of the kk. Therefore, it applies to actions relating to measures which would create the conditions for undertaking an act directly aimed at one of the above mentioned offences. The legislator, within the framework of an act of perpetration, has included the widest possible range of behaviours in order to cover the provision of Article 165a of the Penal Code that could be considered as a manifestation of financing of terrorism or another of the indicated offences.

728. In addition, conduct consisting in making available funds, financial instruments, securities, foreign exchange values, property rights or other movable property or real estate to an organised group or association aimed at committing an offence of a terrorist nature or indicated in the catalogue in Article 165a §1 of the kk, to a person participating in such a group or association or to a person who intends to commit such an offence, was criminalised. In addition, Article 165a of the Penal Code provides for the criminalisation of conduct consisting in covering costs related to meeting the needs or performing the obligations of the group or association or a person referred to in §2 of that article. The scope of this provision excludes persons who are obliged to cover the above mentioned costs or liabilities - in their case, this obligation results from the Act (e.g. maintenance obligations). In that case, the act of committing a terrorist offence consists in "...providing funds for the livelihood of persons, groups or associations which finance committing of terrorist offences. Criminalised activities are activities that satisfy the daily needs and financial liabilities of those groups that support terrorist activities. The purpose of introducing penal sanctions in relation to such acts is to deprive those who support terrorism of financial aid. It is a clear indication to the public that providing a livelihood for those who support terrorism is illegal".[349]

729. Among terrorist organisations, considerable diversity in terms of their size and nature is visible. There are complex terrorist structures, operating like corporations and next to them there are small, decentralised and often autonomous networks. Apart from the organisation, the so-called "lone actors" also exist. The funding requirements for each of the above mentioned

---

[347] http://orka.sejm.gov.pl/Druki6ka.nsf/0/387E14C98A33D8BFC125755A004AE7DC/$file/1660.pdf, date of reading 29 May 2019

[348] Penal Code. Commentary: ed. prof. dr hab. Alicja Grześkowiak, prof. dr hab. Krzysztof Wiak, Publisher: C.H. Beck, issue VI, 2018

[349] Justification of the Resolution of the Senate of the Republic of Poland of 16 March 2017 concerning the Act amending the Act - the Penal Code and certain other acts - Sejm Paper No. 1382, available at: http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=1382 (date of reading 29 May 2019).

groups are also diversified. After all, financing terrorist activities does not only mean covering the costs of carrying out certain terrorist operations but also ensuring the financing of organisational costs, consisting in the development and maintenance of terrorist organisations and the creation of a favourable environment necessary to support their activities. The cost of carrying out the attack itself is currently relatively low, given the scale of the damage caused by the attack or the cost of the measures used for neutralisation or reconstruction. On the other hand, it is costly to create and maintain a terrorist network (or even a single unit of a terrorist organisation), organise the recruitment of members, administrative costs of planning, purchasing, communication and infrastructure. Substantial financial resources are needed for terrorist organisations to reach out with terrorist ideology to their future members, to train their current members, to propagate among the society, to develop certain views and social behaviour. If cutting off terrorist organisations from the flow of financial resources is successful, a new situation is created where the hostile ideological influence of terrorist organisations on the society and on individuals is prevented and the practical possibilities for such organisations to carry out attacks are significantly reduced.

730. The basic legal act in the area of counteracting money laundering and financing of terrorism is the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. The Act in question indicates the authorities and entities operating under the Polish system for counter-terrorist financing and defines their responsibilities and powers.

731. The above mentioned Act defines numerous obligations of the GIFI, the obligated institutions and cooperating units, especially with regard to cooperation and information exchange. Among others, in order to prevent terrorism and financing of terrorism, the obligated institutions apply specific restrictive measures against persons and entities indicated in lists published in the Public Information Bulletin on the website of the minister competent for public finance. Similar to obligated institutions, cooperating units shall immediately notify the GIFI of suspected committing of a financing of terrorism offence. Moreover, on request of the GIFI, they provide or make available within the scope of their statutory competence any information or documents held. In addition, the Border Guard and heads of customs and tax control offices provide the GIFI with information derived from the declaration on the transportation of cash across the EU border.

732. The GIFI verifies the suspicions of financing of terrorism contained in the reports and notifications on the basis of information obtained from obligated institutions, cooperating units as well as foreign financial intelligence units (foreign FIUs). In the case of a justified suspicion of financing of terrorism, the GIFI shall notify the competent prosecutor who, in cooperation with law enforcement agencies, shall take action to prosecute the suspects.

733. Due to the international dimension of the financing of terrorism crime, the GIFI exchanges information with foreign financial intelligence units (i.e. foreign FIUs). On a justified request from a foreign FIU, the GIFI may allow for the provision of information made available by it to other authorities or foreign FIUs or the use of such information for purposes other than those related to the tasks of the FIUs. Similarly, the GIFI also may apply to foreign FIUs for permission to provide information received from it to courts, prosecutors and other cooperating units, other foreign FIUs or to use such information for purposes other than the performance of its tasks.

734. The GIFI may also require the suspension of the transaction or blocking of the account on a justified request of the foreign FIU "allowing for confirming the probability of suspicion of money laundering or financing of terrorism" (pursuant to Article 113(4) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*).

735. In 2018, the GIFI initiated 41 analytical proceedings related to transactions which potentially could have been related to financing of terrorism and 9 proceedings concerning entities subject to specific restrictive measures. Analytical proceedings related to transactions that could potentially be related to financing of terrorism were carried out on the basis of notifications from obligated institutions and cooperating units and on the basis of information or requests received from foreign financial intelligence units. The verification in analytical proceedings usually referred to such transactions which were executed by natural persons coming from countries suspected of supporting terrorism, in the territory of which terrorist groups are active, and countries in the territory of which military actions are performed. Information on transactions of business entities operating in the armaments industry was also analysed. Among others, transactions with entities linked by equity with companies entered in the lists of entities subject to financial sanctions raised doubts. The GIFI cooperated in this scope with the competent authorities mainly in relation to verification of weapons sales transactions in international trade when transferring of weapons in favour of terrorist organisations or infringement of international obligations regarding the failure to make funds available to specific entities was suspected. Moreover, the verification covered, in particular those transactions for which it was difficult to determine the economic substantiation and transactions of foundations associated with Muslim countries concerning which the GIFI received information that they may potentially finance terrorist organisations. On the other hand, the proceedings concerning entities subject to specific restrictive measures were those against persons and entities designated in lists announced by the General Inspector pursuant to the Resolution of the United Nations Security Council, issued under Chapter 7 of the United Nations Charter, related to threats for international peace and security caused by terrorist attacks, in particular, in lists referred to in paragraph 3 of Resolution 2253 (2015) of the United Nations Security Council and in paragraph 1 of Resolution 1988 (2011) of the United Nations Security Council.

Since July 2018, lists of entities to be subject to specific restrictive measures have been published and updated on the GIFI website. In 2018, the GIFI received 1 notification of asset freezing by an obligated institution and 5 pieces of information on transactions involving entities whose names or surnames coincided with the names or surnames of entities on sanction lists or relations with these entities. In addition (under the provisions of *the Act of 16 November 2000 on the prevention of money laundering and financing of terrorism*), the GIFI issued one exemption decision from freezing of assets.[350]

736. According to the information available, the threat of financing of terrorism on the territory of the Republic of Poland, as well as the terrorist threat itself, is currently low. At the same time, however, Poland may be considered as an attractive country for building logistical and financial facilities by terrorist organisations due to its good location, membership in the

[350] Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, pp. 43-45 and 89.

Schengen Area, the alleged lower counter-terrorist regime, etc. With this in mind, the ABW verifies signals on possible provision/transfer of funds for financing of terrorism purposes which are received by the Agency from partner services and institutions or obtained in the course of its operational work. The information thus obtained mostly relates to transfers made through financial institutions or the *Hawala* system. However, due to the nature of the phenomenon, it is difficult to confirm the actual involvement of a person/entity in financing of terrorism.

737. Despite the existing differences between terrorist groups and even within terrorist organisations, there is always a widespread need to hold the financial means to be able to turn the organisation's plans into concrete terrorist acts. The financial resources held by terrorist organisations allow them to support and carry out the full range of activities in which they are involved. Typically, terrorist organisations use the funds obtained for six main purposes, including: terrorist operations; propaganda; recruitment of new members; training of members; remuneration or compensation of members; and providing living conditions for members and their families. The financing of terrorism methods themselves used to generate revenue for terrorist organisations often have regional characteristics and may include: kidnapping for ransom; extortion; funding by charities; cigarette and tobacco smuggling; second-hand car sales; drug trafficking; sale/smuggling of cultural goods; smuggling of natural resources; collection of local taxes, etc.

738. In the context of identifying terrorist networks, terrorist organisations or individual terrorists, traceability of financial operations is important. Since 2010, *the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Programme* has been in force (OJ L 195/5. 27.07.2010). Under the Terrorist Finance Tracking Programme (TFTP), initiated in 2001, the U.S. Treasury Department seeks to identify, track and pursue terrorists and their funding entities. Under the terms of the above-mentioned Agreement, in order to obtain the necessary data from the EU, the U.S. Treasury Department shall submit a request to the designated provider of SWIFT[351] in the United States and provide it with any additional documents. The Department shall simultaneously forward copies of these documents to Europol. According to the agreement, Europol, as the European public authority, assesses whether the data required in a particular case are necessary to combat terrorism and its financing. Europol shall also verify whether each application is adjusted to the requirements arising from the Agreement. Once the compliance of the application with the requirements is approved, the application will have a binding legal force and the designated provider will be bound to provide the required data to the U.S. Treasury Department. Provided data shall be processed solely for the purpose of the prevention, investigation, detection or prosecution of terrorism or its financing. The data provided shall be protected against unauthorised access, disclosure and any unauthorised forms of processing. The search for supplied data shall in any event be carried out solely on the basis of collected information or evidence which indicates that the subject of the search may be associated with terrorism or its financing. The search for the data provided and the reasons for such a search must be documented each time. Downloaded data may be retained only for the period necessary to achieve the purpose for which they were required. The Agreement also lays down guarantees

[351] Abbreviation of the name of the organisation in English - Society for Worldwide Interbank Financial Telecommunication.

to limit further transfer of downloaded data. The U.S. Treasury Department must make TFTP information that may contribute to EU counter-terrorism efforts available to the relevant authorities of the EU Member States concerned, where appropriate, Europol and Eurojust. Similarly, if any additional information is deemed necessary in the U.S.'s fight against terrorism, it must be transferred back[352]

739. In order to examine the potential impact of cash payment restrictions on illegal activities and on the internal market, the European Commission commissioned a study to a private contractor - the consortium established by Ecorys B.V. and the Centre for European Policy Studies. The contractor completed the survey in February 2018.[353] Based on this study, the Commission concluded that restrictions on cash payments would not significantly address the problem of financing of terrorism. The ineffectiveness of this measure stems from the fact that the transactions to which these objectives relate are of too low a value to be covered by the restrictions, or are already illegal transactions which would be slightly affected by an additional ban. By contrast, a ban on high-value cash payments would have a positive impact on combating money laundering. With regard to financing of terrorism, the study concludes that terrorists and criminals make widespread use of cash because it allows them to minimise the risk of detection. Money provides anonymity and makes it easier to hide not only illegal activities but also related legal transactions that could otherwise be traced by law enforcement. Money plays a significant role in many terrorist activities. The survey refers to the argument that since the attacks of 11 September 2001, the costs of carrying out a terrorist attack have been steadily decreasing, they often do not even reach EUR 10,000, which is a fraction of the estimated costs of preparing the above mentioned attacks of 11 September 2001, estimated at USD 400,000 - 500.000. The survey distinguishes between impacts on illegal transactions and impacts on legal transactions. Illegal transactions are transactions that are not compliant with the law (e.g. the purchase of explosives) or seemingly legal transactions where both parties know that they serve illegal activities. Since such transactions were already illegal beforehand and since the parties to such transactions knowingly took the risk of prosecution and criminal sanctions, it seems doubtful that the ban on cash payments was respected or had any deterrent effect. It is unlikely that criminals who already deliberately violate the law will be deterred by an additional ban on payment transactions. This is particularly evident where the sanctions associated with this additional ban are small compared to those for the main criminal activity. Legal transactions are transactions ancillary to the main criminal activity which are not in themselves criminal in nature (e.g. car rental) and where it can be assumed that the counterparty (e.g. a car rental company) is unaware of their criminal purpose (e.g. transport of explosives). In this context, the prohibition to pay in cash could be respected at the initiative of an honest counterparty, with the result that payments for the transaction would be made by other means or there would be no transaction. Unfortunately, in this case, it can be suspected that, due to the legality and prevalence of this type of transactions, paying for them with identifiable means would not necessarily enable the detection of suspicious activity. It should be noted that many

[352] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=LEGISSUM:jl0039rom=EN and https://uodo.gov.pl/pl/p/tftpreading date 2 May 2019

[353] Report from the Commission to the European Parliament and the Council on restrictions on cash payments, Brussels, 12 June 2018, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557325306958ri=CELEX:52018DC0483.

of usual transactions carried out in the preparation of terrorist attacks have recently been paid for by traceable means without raising any suspicion.

740. According to the data obtained from the Ministry of Justice, in 2017 Polish courts initiated single court proceedings under Article 165a of *the Penal Code* against three persons. In the same year, three persons were sentenced in the first instance for an offence under Article 165a of the kk. According to the above mentioned data, in 2018 sentences against three persons convicted of an offence under Article 165a of the kk became final.

741. According to the data contained in the "EU Terrorism Situation & Trend Report 2018", 2 people were arrested in Poland in 2017 in connection with suspected terrorist activity (religiously motivated terrorism). In addition, courts in Poland conducted cases of terrorist crimes against four persons (in cases of religiously motivated terrorism). Three people have been convicted and one acquitted[354]

6.3. MOST COMMON METHODS USED TO FINANCE TERRORISM

742. In order to ensure effectiveness of the fight against financing of terrorism, it is necessary to know, detect and counteract any forms of acquisition, movement and transfer of funds and other assets by terrorist organisations and their supporters and to prevent such practices. It is important to act in such a way that law enforcement authorities can use financial operations to locate terrorists and deter them from committing crimes as far as possible. Counteracting financing of terrorism also involves neutralising the sources of income of terrorist organisations by disrupting the ability of terrorist organisations to raise funds. To ensure the effectiveness of counter-terrorist financing activities carried out by the state authorities, they must target not only terrorists and terrorist organisations but also their supporters. These activities should include, inter alia, foreign terrorist militants, financial supporters and fund-raisers and any other persons who knowingly contribute to supporting terrorist activities. From the point of view of countries combating financing of terrorism, financial intelligence units and tracking systems such as the TFTP are key instruments for detecting financial flows through financial transactions or identifying terrorist networks and their supporters[355]

743. The financing of terrorist activities may take place with the use of funds obtained from legal sources (e.g. the use of charitable organisations or legitimate business activities), through self-financing and the use of criminal activities as a means of fundraising.

744. *Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or financing of terrorism and amending Directives 2009/138/EC and 2013/36/EU* (OJ L 156, 19.06.2018, p. 43), hereafter referred to as Directive 2018/843, explicitly mentions that, on the basis of information from the United Nations, Interpol and Europol, there is a growing convergence between organised crime and terrorism. The Directive states that the links between organised crime and terrorism and the links between criminal and

---

[354] EU Terrorism Situation & Trend Report 2018, Europol, 2018, pp. 55-59, available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018.

[355] Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, Strasbourg, 2 February 2016, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0009.02/DOC_1ormat=PDF.

terrorist groups pose a growing threat to EU security. The terrorist groups in operation turned to alternative sources of funding, including criminal activities long ago. The very use of criminal activities to raise funds for terrorist purposes ranges from petty crime in the form of fraud to involvement in serious and organised crime such as arms trafficking, kidnapping for ransom, extortion and drug trafficking.

745. As stated in the Report on the state of security in Poland in 2016[356], organised crime is usually divided into three areas - economic crime, drug crime and criminal crime. However, some organised groups have a multi-crime nature, i.e. they operate simultaneously in different crime areas. In Poland, the largest area of activity of organised crime groups is economic crime, which causes the highest losses to the state budget and undermines Poland's economic security. On the other hand, with respect to organised crime related to drugs, it should be pointed out that Poland, due to its location at the crossroads of smuggling routes, is both a transit country for drug smuggling and a destination country, as well as a significant producer of synthetic drugs in particular. Foreign trends in the demand for drugs and the availability of precursors for their production have a direct impact on the Polish drug market. At the same time, the above-mentioned report states that organised crime of criminal nature constitutes a relatively smaller threat compared to economic or drug crime.

746. Along the decline in sponsoring of terrorist groups by so-called sponsor countries, drug trafficking and trafficking in psychoactive substances has become an attractive source of funding for terrorist groups. Highly profitable drug smuggling and trafficking makes it possible to raise large sums of money in a relatively short time. The infiltration of both criminal and terrorist figures in terrorist organisations is increasingly blurring the distinction between organisations that only deal in drug trafficking and the terrorism. Criminal organisations and terrorist groups are developing international networks of influence. Globalisation and the opening of borders have enabled both terrorist and criminal organisations to develop and expand their activities. Investigations conducted by law enforcement agencies and intelligence allowed to identify direct links between various terrorist and drug trafficking organisations.

747. Another method of financing of terrorism referred to in FATF reports is credit card fraud[357] It refers primarily to offence related with shopping - via the Internet or by phone - using someone else's credit card details that have been fraudulently obtained. Credit card data is stolen or fraudulent use is made of the market for illegally obtained and sold personal data, including credit card account numbers, other personal information such as the cardholder's name, address, telephone number, card start and end dates, card security number, etc.

748. Tobacco-related crime is also one of the methods of illegal fundraising by terrorist organisations. In Poland, according to data of the National Revenue Administration, the total value of illegal cigarettes disclosed by the National Revenue Administration, the Border Guard and the Police in 2017 amounted to over PLN 369.2 million, while the total value of illegal tobacco products and dried tobacco products disclosed by the National Revenue Administration, the Border Guard and the Police in 2017 was PLN 254.4 million. There is no

[356] Report on the state of security in Poland in 2016, MSWiA, published in October 2017, available at: https://archiwumbip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html.
[357] For example, FATF-GAFI Report - Terrorist Financing, FATF, February 2008, pp. 17-18, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF Terrorist Financing Typologies Report.pdf.

information as to whether the funds from the crime in question have contributed to terrorist funds in Poland.

749. The FATF report *Terrorist Financing Disruption Strategies 2018* mentions smuggling and selling of cultural goods as a method of financing terrorism used to generate revenue for terrorist organisations[358] This is particularly important in the case of ISIS and cultural goods taken out of Iraq and Syria. According to Internet data[359], ISIS annual revenue from the smuggling and sale of cultural goods is estimated at the level of at least USD 100 million. Sales take place not only on the illicit market but also on official websites such as eBay.

750. *Communication from the Commission to the European Parliament and the Council on an Action Plan to combat terrorist financing more effectively* (Strasbourg, 2 February 2016) COM(2016) 50 final) identifies offences related to illegal trade in wildlife as a current source of financing of terrorism and related activities. According to the data contained in the EU Action Plan against illegal wildlife trade,[360] illegal wildlife trade has now become one of the most lucrative types of organised crime worldwide. The exact scale of this crime is unknown, but various sources estimate the profits from this crime at between EUR 8 and 20 billion per year. It refers to a wide range of protected species, including elephants and rhinos, corals, scales, tigers and great apes.

751. Another way to raise funds cited in the literature is extortion. This crime is committed by individuals who are members of expatriate communities and at the same time identify themselves with the aims of terrorist activity in the diaspora. A terrorist organisation taxes the income and savings of the diaspora and enforces the tax imposed. Extortion is generally targeted against own community, where there is a high level of fear of revenge if anyone informs the authorities. Terrorist organisations can also threaten to harm relatives who stay in the victim's country of origin, which further increases the lack of reports of illegal activities to law enforcement authorities. Extortion from community members in the diaspora can be a significant and permanent source of funding for terrorist activities.

752. An important source of raising funds for terrorist activities is the collection of taxes or other charges. This was particularly important in the case of ISIS, where withdrawals from bank accounts or the use of vehicles transporting goods were taxed. Dissenters were additionally taxed with *jizza*, a fee/tax for release from military service and defence by the Muslims and the privilege of living on the Muslim territory. Currently, attempts to introduce *jizza* have been reported in Egypt and numerous cases of extortion of *jizza* were reported in British prisons where Muslim criminals collected tribute from fellow prisoners of other faiths. The so-called revolutionary tax was also collected by the ETA, the separatist terrorist organisation of the Spanish Basques.

753. Another form of raising funds for terrorist activities is *kidnapping*. In 2008, the victim of the kidnapping was a Polish engineer-geologist residing in Pakistan as an employee of PGNiG Geofizyka Kraków company. The kidnappers have sent demands for the release of more than

[358] Terrorist Financing Disruption Strategies 2018, FATF, October 2018, p. 11.
[359]eg.http://www.psz.pl/124-polityka/jak-panstwo-islamskie-stalo-sie-najbogatszym-ugrupowaniem-terrorystycznym, date of reading 2 May 2019
[360] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - An EU Action Plan against illegal trade in wildlife, available at: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016DC0087rom=pl.

100 Taliban and the withdrawal of military forces from the Pakistan-Afghan border region. Later, they softened their position by pressing for a tribute to be paid to them in exchange for releasing the Pole. Unfortunately, negotiations with the terrorists did not succeed and the Pole was decapitated. Several cases of kidnapping of Polish auxiliary personnel serving on ships have occurred in recent years on waters around the Horn of Africa and the Gulf of Guinea. The actions of pirates should not be directly identified with terrorist attacks. However, the existence of links between some pirates and terrorist organisations active in Somalia or Nigeria has been noted.

754. To fund terrorist activities, terrorist organizations receive substantial support and funds from and through legitimate entities, including income from the business activities of economic operators, donations (victims) from the ethnic groups from which their members come from, compensation for the work of their members or henchmen, the sale or rental of property, raising of credits and/or loans and material assistance from the family, charitable collections or government subsidies, savings or benefits of their members or henchmen.

755. Charitable organisations play an important role in this case. These organisations benefit from public trust, have access to significant and diverse sources of funding and their financial activities are often characterised by high cash flow. Some of the charities are known in many countries and operate practically all over the world, often in areas of conflict. This provides a framework for conducting national and international financial operations and transactions, often in or near areas most vulnerable to terrorist activity. At the same time, charities - as non-profit organisations - are subject to much softer regulatory requirements than financial institutions or trading companies (this applies to capital requirements, certificates of professional competence, current accounting, reporting and monitoring). Among the ways (methods) used to collect and transfer funds designated for terrorist activities using charitable organisations, the following methods can be specified:

1) Re-directing funds through fraud. In this case, the charity organisation acts and performs its tasks in accordance with its statutory objectives. However, some of the funds raised by the charity organisation are misused and transferred for terrorist purposes. In such a case, the charity organisation may act as a façade organisation for the collection of funds intended for terrorist purposes, while at the same time performing the important social functions for which it was established. As a rule, the misappropriation of funds is carried out by few people in the charity organisation who have privileged access to these funds.
2) Using a completely fictitious or fraudulent organisation claiming to be a legitimate charity as a façade organisation for terrorist groups. In such a case, the funds obtained from all sources by the charity are transferred for terrorist purposes and donors - who have contributed funds being aware that their donations are intended for non-terrorist purposes - are not aware of the use of their funds in connection with financing of terrorism.
3) So-called broad use - this is the case when a charity acts in accordance with its statutory tasks, carrying out activities that are socially useful and for the benefit of society but acts through a well-known terrorist organisation. The purpose of activity of the charity organisation is therefore also to support a terrorist organisation.

756. Terrorist activities (whether closely related to terrorist activities, logistics or recruitment) can also be financed by funds originating from legitimate business activities. Income from legal activities comes primarily from those sectors of the economy where there are no formal

qualification requirements (such as master's certificate, license) at the start of the activity and where starting the activity does not require significant investment. The risk that the company will redirect funds to support terrorism is greater when the relationship between recognised sales and actual sales is difficult to verify and in the case of capital intensive activities. However, the example cited most often in the literature is the international network of companies belonging to Osama bin Laden, which is an example of the link between legal economic activity and the use of its revenues for terrorist purposes.[361] The network included, among others: a construction corporation, transport companies, an ostrich farm, a bank, shrimp ships, oil factories, confectionery factory, diamond mines and many others.

757. The financing of terrorist activities may also originate from internal sources, including family financing, income from self-employment and other non-criminal sources. The amounts of money needed to carry out small attacks can be collected by individual terrorists and their support networks using savings, access to credit or other profits from activities controlled by them. Terrorist organisations can be highly decentralised and self-financing can also include cases where funding is provided by an autonomous external factor that is not directly involved in the planning or implementation of an attack, despite the provision of funds for that purpose.

758. According to the information available, until early 2019 while carrying out its operational and analytical activities, the ABW noted the following methods of raising funds in Poland with the purpose of supporting terrorist organisations:

- income from work (legal and illegal);
- financial support from family members;
- collections conducted under the guise of charity support (including online);
- collections conducted on behalf of a terrorist organisation (voluntary and forced);
- proceeds from criminal activities (smuggling, fraud, extortion, etc.).

759. Moreover, the ABW has also recorded cases of investing on the territory of the Republic of Poland of funds obtained by members and supporters of terrorist groups, including related economic entities (or in order to establish further ones), whose income is then allocated to a given organisation, as well as the purchase of real estate by these persons (including without economic justification - e.g. in a poor technical condition).

760. As regards the movement of funds raised for terrorist purposes, the FATF report of 29 February 2008[362] on Terrorist Financing lists three main methods for the movement of money and value by terrorists. The first method is the use of the financial system, the second one requires physical movement of money (for example through the use of *cash couriers*) and the third method uses the international trading system. On the other hand, the FATF report of 2018 - *Terrorist Financing Disruption Strategies 2018* includes the following mechanisms among the main mechanisms used by terrorist groups to transfer funds: the banking sector; crowdfunding; MVTS, including Hawala; prepaid cards; trading in high-value goods; virtual currencies and other digital media; and physical transportation of cash[363]

[361]For example, Brunon Hołyst, Terrorism. Volume 1, ed. LexisNexis, Warsaw 2009
[362]For example, FATF-GAFI Report - Terrorist Financing, FATF, February 2018, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF Terrorist Financing Typologies Report.pdf.
[363] Terrorist Financing Disruption Strategies 2018, FATF, October 2018, p. 11.

761. As modern terrorism is made up of diverse organisational structures, there is also a constant evolution of techniques used in response to international efforts to counteract this phenomenon. Although it is difficult to determine which of the techniques is the most common method of transferring money for terrorist purposes, the use of the banking system seems the most convenient from the point of view of the activities of terrorist organisations. In this way, activities that are closely related to terrorist activity can be easily financed, including logistical or recruitment activities. Money can be transferred through the banking system both within one country and from one country to another. Funds transfer transactions may be concealed through accounts held for a false name, charity organisations or companies, in order to hide the final recipient. The use of a bank account to transfer funds can take the form of transferring both legal and illegal funds to countries of conflict or countries bordering countries where terrorist organisations operate. Funds are often transferred to accounts with credit institutions located in jurisdictions that do not comply with international AML/CTF standards and recommendations. Bank accounts belonging to individuals linked to terrorists (family and other relatives) may be used for cash deposits and subsequent cross-border transfers. Self-financing of terrorists also occurs especially the "lone wolves") from their own funds, accumulated in a bank account (often from totally legal sources - earnings, credits/loans, scholarships, family donations).

762. In accordance with one of the definitions, *crowdfunding* is a type of accumulation and allocation of capital provided for the development of the specific undertaking in exchange for the specific return benefit which involves a wide range of capital providers, is characterised by the use of ICT, a lower entry barrier and better transaction conditions than those generally available on the market. When funds are collected and transferred for terrorist activities, the actual purpose of the collection will not directly indicate an intention to use the funds accumulated for financing of terrorism. The organisers of the collection (supporters of the terrorist organisation) send out appeals for funds through applications such as Twitter. After finding the willing persons, they are also contacted by an instant messenger e.g. via Skype. Donors make cash donations to the initiators of the action or buy international telephone prepaid cards, whose numbers they subsequently make available to them.

763. Alternative money remittance systems, operated in the EU by payment service providers under the relevant legislation, are also used for moving funds for terrorism-related purposes. The use of alternative remittance systems is rooted in weaker or less clear accounting and less stringent regulatory oversight. The level of anonymity in relation to banking products is also increased.

764. Another type of alternative system for transferring funds used by terrorist organisations for reasons of anonymity, convenience, speed and availability is the informal financial system called *Hawala* or *hundi*. The term *Hawala* itself is derived from Arabic and means a transfer or remittance, originally used by merchants in South Asian countries for the safe transfer of money. The essence of the *Hawala* system is to act on the principle of compensation and to rely, solely on the basis of trust, between the participants in the system. *Hawala* transfers were made, inter alia, during the preparation of the attacks on the World Trade Center and Pentagon in 2001. Today, the *Hawala* system is based on a network of intermediaries called *hawaladars* or *Hawala* banks, usually operating unofficially, under the cover of other business activities, e.g. travel agencies, exchange offices, laundries, restaurants, kebab bars, forwarding companies etc. Pakistan, India and the United Arab Emirates are significant centres of activity of *Hawala* intermediaries. The *Hawala* intermediary, in fact, runs an underground bank, lending, accepting

deposits and making transfers all over the world, practically without using the official banking system, using single passwords, for example quotations from the Koran, names, agreed words or the code of digits which the depositor in one country indicates to the intermediary and the recipient of money in another country provides on receipt of the sum transferred in this way. The most important feature of the *Hawala* system is the speed of transfers, anonymity, the ability to transfer virtually any amount, the absence of any formalities or documents and remaining completely invisible to the official banking system. Cost effectiveness, reliability and tax avoidance are also important. The 2013 Report of the Financial Action Task Force indicates the existence of different types of *Hawala* intermediaries, ranging from those operating officially, to the extent possible, to the hybrid model, often remaining invisible to the relevant services and the typical criminal and illegal model of intermediaries. *Hawala* transactions are performed immediately after accepting cash by the intermediary and providing the password. When accepting cash from the payer, the intermediary immediately orders the withdrawal of funds in another country by fax, e-mail, phone call, chat, social networking site entry, Internet advertisement or in any other way that does not raise any suspicion. The accepted money is not transferred through the banking system and the compensation of the money is performed on a two-pot basis. The two-pot rule is based on the principle that against the amount accepted from the depositor, the intermediary will subsequently make withdrawals since he does not have to physically transfer the money to another intermediary immediately. The debt will be offset when the sum of deposits and withdrawals from intermediaries is balanced. The whole idea is based on trust between intermediaries and possible compensation of the difference occurs every few years. Compensation can be made by means of couriers. Couriers of the *Hawala* system usually do not carry cash but only gold, diamonds, valuable antiques, which can converted into cash by intermediaries immediately after the transportation. An important element of the informal banking system is the ability to maintain full anonymity of both the payer and the payee and to use several intermediaries when ordering transfers. In this way, the *Hawala* bank usually does not know from whom, for what and to whom it is trading, so it can even remain uninvolved in the international terrorism system. The most important aspect is trust between intermediaries. Informal banking does not leave visible traces indicating performing of the transaction. Moreover, the cost of making a transaction is much lower than in a traditional bank. Money transferred by the *Hawala* Bank can reach the most remote village in India, Pakistan or Afghanistan, even where there are no legally operating banks. *Hawala* is widespread in Western Europe, especially in Germany, France and the United Kingdom there are many intermediaries offering underground banking services. It is associated with the large groups of immigrants from the Middle East, India, Pakistan and the Philippines staying in these countries.[364]

765. Due to the fact that countries and international organisations increasingly undertake new measures to counter terrorist financing, especially with a view to applying security measures in the official financial system and creating a real and effective barrier to the movement and acquisition of these funds, the physical movement of cash by means of courier is one of the ways used by terrorist organisations to move their funds. In this way, they omit the safeguards established under the International Standards against Money Laundering and Financing of terrorism in financial institutions. Terrorist organisations using couriers to transfer funds for terrorist purposes often swap money for other values, e.g. gold bars (or jewellery, expensive

[364] http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu/, date of reading 10 May 2019

stones, etc.) to move assets outside the financial system. Terrorists can store their assets, e.g. in gold since its economic value is easy to determine and remains relatively fixed over time. Moreover, given the cultural importance of gold in many areas of the world, for example in South-East Asia, South and Central Asia, the Arabian Peninsula and North Africa, there will always be a demand for gold. Counter-terrorism activities carried out in many countries have shown that money couriers transferred funds to a number of countries in the Middle East and South Asia. Direct air routes are used for simple transfers; however, in more complex fund transport plans there are indirect air routes with the use of multiple cash couriers and changes in currencies. Moving money for terrorist purposes by courier services across borders is predominant in countries where e-banking systems are underdeveloped or their use by the population is limited. In the major part of Africa and the Middle East, communities rely mainly on cash, which contributes to the use of couriers or alternative remittance systems. The analysis of a number of terrorism cases has revealed that money couriers are also active in Europe, even in countries with well-functioning financial systems. In the majority of cases, couriers are involved in moving funds generated and maintained outside the financial system to avoid detection. Moving funds with the use of money couriers can be relatively expensive compared to bank transfers. However, as legitimate financial institutions tighten their procedures and apply due diligence, the use of couriers has become an attractive method of transferring funds without leaving a transaction trail. The amounts of cash transported by terrorist organisations for terrorist purposes as such can be very low which hinders their detection and enforcement of bans/restrictions on cross-border transport. Couriers also leave no audit trail for law enforcement agencies.

766. Another way to move funds for terrorism-related purposes may be the use of virtual currencies. In Poland, *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* contains a definition of a virtual currency and defines it as a digital representation of a value that is not:

- a legal tender issued by NBP, foreign central banks or other public administration bodies,
- an international unit of account established by an international organisation and accepted by individual countries belonging to this organisation or cooperating with it,
- electronic money within the meaning of the *Act of 19 August 2011 on payment services*,
- a financial instrument within the meaning of the Act of 29 July 2005 on trading in financial instruments,
- a promissory note or a cheque

and which is exchangeable in business transactions to legal tender and accepted as the means of exchange as well as can be electronically stored or transferred, or can be subject to electronic trade.

767. In a more popular sense, virtual currencies include cryptocurrencies and some other contractual units that can be exchanged for regular money, such as the currencies in some computer games. Virtual currencies can be used to move assets for terrorist purposes due to their characteristics that are conducive to the anonymity of the parties to a transaction and make it difficult both to track transfers and to stop them. EUROPOL's analysis of 19 September 2017

(*Risk Analysis on the use of Virtual Currencies for Terrorism Financing purposes*) concluded, however, that while virtual currencies gained in popularity due to key features such as global availability, ease of access, reliable and irreversible transactions, low cost and high speed of international transfer, their popularity in terrorist organisations seems relatively low compared to the popularity of transnational organised crime groups, especially those related to cybercrime. The number of known or identified cases of using virtual currencies for financing of terrorism purposes remains very low. The number of signals in Poland concerning the possibility of using virtual currencies for financing of terrorism is also small.

768. Prepaid cards are also used to move funds for terrorism-related purposes. The risk of using this product for financing of terrorism results mainly from its anonymity and the possibility for third parties to charge accounts associated with it (e.g. by transfer to a technical account). The *Communication from the Commission to the European Parliament and the Council on an Action Plan to combat terrorist financing more effectively* argues that prepaid cards have important advantages as instruments to prevent social exclusion. Under Polish conditions, in 2015, the Polish Financial Supervision Authority, as a result of its supervisory activities, prohibited issuers (banks) under the KNF (PFSA)'s jurisdiction from issuing and servicing prepaid cards, justifying it by a very conservative treatment of electronic money and its relation with prepaid cards. In the KNF (PFSA)'s opinion, a prepaid card should not be treated as electronic money which affects the banks' obligations in the scope of issuing and servicing prepaid cards. As a result of the supervisor's actions, there are currently several dozen pre-paid card issuers on the Polish market, which operate in our country on the basis of a single European passport and Polish issuers are prohibited from conducting such activity. However, from the point of view of competition of Polish banks with banks from other Member States, it is important that in other Member States prepaid cards for which a technical account is kept, are recognised as electronic money (among others, in Hungary, Italy, the United Kingdom)[365]

769. At the same time, according to the information available to the ABW, as a result of its operational and analytical activities, the ABW recorded the following methods of transferring the accumulated funds outside the Republic of Poland:

- through the banking systems;
- with the use of cash transfer intermediaries;
- through the *Hawala* system;
- through couriers.

770. One of the basic tasks of the prosecutor's office is to prosecute crime, including, inter alia, offences related to financing of terrorism. Below, 3 examples of conducted preparatory proceedings in this scope are presented.

<u>Example no. 1.</u>

While carrying out this task, the Department for Organised Crime and Corruption of the National Prosecutor's Office conducted an investigation, concluded by the act of indictment, against three citizens of the Russian Federation of Chechen origin suspected of participating in an organised group with the aim of committing terrorist offences and financing them.

[365] Position of the Government of 25 March 2016 concerning the *Communication from the Commission to the European Parliament and the Council on an Action Plan to combat terrorist financing more effectively*.

Financing of terrorism in this case consisted in collecting tribute among the local Chechen diaspora in the form of donations for religious purposes and transferring it in cash, through couriers, to the fighters of the so-called Caucasus Emirate which carries out terrorist activities on the territory of Russia, aimed at creating a fundamentalist Islamic state in the North Caucasus, based on the Sharia law. Another revealed form of financing terrorism was the purchase, through the citizens of the Republic of Poland, of paramilitary equipment and then sending it by mail to the area adjacent to the theatre of armed activities conducted by terrorist organisations. The accused did not confess to the alleged acts and stated that although the money had been collected, it was transferred to the independence activities of Chechen fighters struggling for the Chechen Republic of Ichkeria. Three defendants were sentenced to two years and one month's imprisonment by the Regional Court in B. in August 2017. The fourth of them was acquitted. The Court of Appeals in B. disregarded the appeals and upheld the judgement issued in force.

Example no. 2.

The Department of Organised Crime and Corruption of the National Prosecutor's Office is investigating financing of terrorist activities involving the receipt by persons of Middle Eastern nationalities of funds from relatives or related persons of ISIS fighters residing in Member States of the European Union, and the subsequent transfer of those funds through the Hawala underground banking system directly to those combatants residing in war zones. The operator of one of the money transfer systems whose outlets were opened in branches of Polish banks, was used to receive money by hawaladars in Poland.

Example no. 3.

The Department of Organised Crime and Corruption of the National Prosecutor's Office is investigating the financing of one of the organisations listed in the Council Implementing Regulation (EU) No. 2017/150 of 27 January 2017 by members of one of the national minorities living in Poland. Financing took place through the collection of donations called "revolutionary tax" among the members of the above-mentioned diaspora who were running business. The money was exported by couriers from Poland to another EU Member State where it was distributed by the regional management of the terrorist organisation. In addition to allocating the funds collected for peaceful manifestations of the organisation's activities, the money collected was also used to finance terrorist activities in one of the countries of the Middle East.

7. VULNERABILITY TO MONEY LAUNDERING AND FINANCING OF TERRORISM

7.1. VULNERABILITY IN THE SCOPE OF LEGAL REGULATIONS

771. The issues of vulnerability to money laundering and financing of terrorism may be considered primarily in 3 areas. The first one relates to generally applicable rules, in particular as far as they govern the functioning of the national anti-money laundering and counter-terrorist financing system, including the activities of financial and non-financial institutions offering products and services related to the risk of money laundering and financing of terrorism as well as the supervision and control of those institutions.

772. The second area relates to issues associated with the functioning of the economy, in particular the business practice of financial and non-financial institutions offering products and services that may be associated with the risk of money laundering and financing of terrorism. In this case, it is essential whether these institutions make every effort to ensure that this risk is mitigated through the due application of the existing provisions of common law as well as their internal procedures. This area also raises the issue of assessing whether the supervision of these financial and non-financial institutions is adequate.

773. In addition, the possibilities to prevent and combat money laundering and financing of terrorism under the national anti-money laundering and counter-terrorist financing system are also important. This issue relates primarily to the effectiveness of the functioning of public administration bodies under the national anti-money laundering and counter-terrorist financing system.

774. In the case of considering vulnerability under the existing legislation, it should be borne in mind that the risk of money laundering and financing of terrorism is affected both by legislation directly relating to the prevention and counteracting money laundering and financing of terrorism and by other legislation relating to the functioning of various elements of the national anti-money laundering and counter-terrorist financing system or the absence thereof.

775. The adoption in 2018 of *the Act of 1 March 2018 on counteracting money laundering and* changed not only the legal basis for the national anti-money laundering and counter-terrorist financing system but also provided opportunities to improve its functioning. The main objectives of this change were as follows:

- implementation of the provisions of Directive 2015/849 (in addition to other EU legislation[366]);
- adjustment to the FATF recommendations revised in 2012;
- implementation of the recommendations of the evaluators from the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL, which were indicated in the report issued in 2013 after the evaluation of the Polish anti-money laundering and counter-terrorist financing system carried out in the fourth evaluation round of Member States.
- achieving a more effective anti-money laundering and counter-terrorist financing system based on practical experience in the scope of application of former legislation (i.e. *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism*).

776. Fundamental changes introduced by the Act of 1 March 2018 on *Counteracting Money Laundering and Financing of terrorism* included:

- restructuring of the catalogue of obligated institutions[367];
- establishment of a Financial Security Committee with broader powers than the former Inter-Ministerial Financial Security Committee;
- indicating mechanisms concerning preparation of opinions on the national risk assessment of money laundering and financing of terrorism;
- specifying the detailed obligations of the obligated institutions, including in the scope of application of customer due diligence measures;
- introducing a legal basis for the establishment and operation of the Central Register of Beneficial Owners;
- improving the rules concerning the collection by the GIFI of information necessary for the performance of its statutory tasks, their protection and making this information available to other entities;
- amending the provisions concerning suspension of transactions and blocking of accounts;
- introducing the precise definition of the rules of cooperation between the GIFI and foreign financial intelligence units and Europol;
- improving the provisions concerning the application specific restrictive measures against persons, groups and entities;

[366]In particular, *Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities* (OJ L L 342, 16.12.2016, p. 1) as well as the provisions of *Directive 2018/843* drafted during the preparation of the law.

[367]The catalogue of obligated institutions has been expanded by entities indicated in the applicable regulations in Article 2(2)(12), (16), (24) and (25) of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*. Its change also consisted in rebuilding the content of other paragraphs in the above mentioned provision with regard to some other categories of obligated institutions.

- amendment to the regulations regarding the control of obligated institutions as well as administrative sanctions imposed on obligated institutions which fail to comply with the obligations imposed thereon by this Act.

777. The *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* has been adopted relatively recently. Not all of its provisions came into force as of 13 July 2018. For some provisions, a longer *vacatio legis* is foreseen - they will enter into force in the second half of 2019, in particular the regulations on the Central Register of Beneficial Owners will apply from 13 October 2019.

778. *The Act of 1 March 2018 on counteracting money laundering and financing of terrorism* contains statutory delegations requiring issuing of 9 implementing regulations. By the end of May 2019, 6 of them, referred to in Article 62 and 71, Article 78(3), Article 80(3), Article 85(4) and Article 134(2) of the aforementioned Act were adopted and published. Drafts of 3 subsequent regulations (i.e. those indicated in Article 79(3), Article 84(4) and Article 84(4) of the aforementioned Act) have been prepared[368]. Article 109 of the above mentioned Act additionally indicates a statutory delegation which gives the possibility of an optional regulation issued by the minister competent for public finance concerning preparation and acceptance by the GIFI of applications from cooperating units (in the mode provided for in Article 104(1) and Article 105(1), (3) and (4) of the above mentioned Act), the mode of their acceptance as well as the provision by the GIFI of the information referred to in Article 106 (1) and (2) of the above mentioned Act.

779. With regard to the catalogue of obligated institutions contained in *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, it should be noted that in the transnational risk assessment of money laundering and financing of terrorism, the European Commission indicated that Member States should also include such types of entities as: *crowdfunding* entities, auction houses, entrepreneurs trading in works of art and antiques as well as other high value goods[369]

780. On the other hand, Directive 2018/843 - the implementation of which is being prepared[370] - introduces an obligation to cover the following entities under the regulations on counteracting money laundering and financing of terrorism:

- other persons (i.e. not only statutory auditors, external accountants and tax advisers) who undertake to provide, directly or through other persons with whom they are linked, material assistance, support or advice on tax matters in the course of their main business or professional activities (Article 1(1)(a) of Directive 2018/843);
- persons trading in works of art or acting as intermediaries in the trade in works of art, including where such trade is conducted by art galleries and auction houses, if the

[368] As of 27 May 2019, they were already agreed upon internally.
[369] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 26 June 2017, p. 18, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.
[370] As of 28 June 2019. However, some of its provisions - mainly concerning "entities providing currency exchange services between virtual and fiduciary currencies" and "providers of virtual currency accounts", as well as the limits in case of the failure to apply customer due diligence measures (i.e. financial security measures) to the customer with regard to electronic money - have already been reflected in the provisions of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing.*

value of the transaction or a series of related transactions is EUR 10,000 or more (Article 1(1)(c) of Directive 2018/843);

- persons storing works of art, trading in works of art or acting as intermediaries in the art trade, where such activity is carried out through *free ports*, if the value of the transaction or a series of related transactions is EUR 10,000 or more (Article 1(1)(c) of Directive 2018/843).

781. The analysis of the content of Directive 2018/843 shows that apart from the changes in the catalogue of obligated institutions and certain modifications of some of the definitions used, among others, the following provisions should be implemented in the Polish legal order:

- modification of application of the customer due diligence measures;
- publishing and updating a list of positions identifying politically exposed persons;
- detailed specification of the rules for maintaining the Central Register of Beneficial Owners, including in the scope of data verification, data storage, penalties for failure to obtain and possess by corporate and other legal entities accurate and up-to-date information on their beneficial owners, integration of the register with registers of other EU countries through a European central platform[371];
- detailed specification of the scope of statistics needed to review the effectiveness of the system to counteract money laundering or financing of terrorism;
- registration of entities providing services in the area of virtual currencies;
- exchange of information and assistance between the competent authorities of EU Member States without providing for exceptions to refuse information or assistance;
- establishing a centralised automatic mechanism such as the central register or the central electronic data retrieval system which allows for the relatively rapid identification of any natural or legal person holding or controlling payment accounts and bank accounts and safe deposit boxes[372].

782. In early 2019, the European Commission sent a "supplementary justified opinion" concerning the failure to notify measures transposing Directive 2015/849 into the national law. It indicates - in 48 paragraphs - the shortcomings in the implementation of the aforementioned EU legal act. After their in-depth review, inter alia as part of the work of the Financial Security Committee, a reply had been prepared in which it was stated that, in the opinion of the Republic of Poland, the provisions of Directive 2015/849 had been correctly transposed into the national legal system in the vast majority of cases and detailed explanations were provided in relation to each of the paragraphs indicated in the "supplementary justified opinion". In the opinion, it was emphasised, among others, that the doubts raised by the European Commission regarding the implementation of the provisions of Directive 2015/849 may originate from insufficiently

---

[371] Indicated in Article 22(1) of *Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 on certain aspects of the company law* (OJ L 169, 30.06.2017, p. 46).

[372] Work on creating a legal basis for establishing and functioning of such a centralised mechanism started in Poland several years ago. In December 2016, a draft *Act on the Central Database of Accounts* was sent for external arrangements and consultation. In connection with the need to implement Directive 2018/843, work on the above project is to be continued along with the development of provisions implementing other provisions of the aforementioned Directive.

precise information about the adopted transposition measures submitted to the European Commission. It was pointed out that due to the legal provisions already in force in Poland, including directly applicable EU law or the case law of national courts, some of the provisions of Directive 2015/849 did not require additional legislative action as it was already reflected in national law.

783. It should be noted that in July 2018 the MONEYVAL Committee adopted Poland's report under Step 1 of the *compliance enhancing procedure* (CEP), based on an analysis prepared by the MONEYVAL Secretariat which stated that *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* eliminates most of the shortcomings identified in the fourth round of mutual evaluations. The MONEYVAL Committee concluded that Poland brought the transposition of all outstanding key and relevant recommendations to a "largely consistent" level. Thus, the conditions for excluding our country from the CEP process have been met. In connection with the results of the Secretariat analysis and after the discussion of the report, the Plenary Meeting concluded that Poland had taken sufficient steps to remove it from the CEP procedure.[373]

784. As regards the criminal provisions penalising money laundering and financing of terrorism, i.e., Articles 299 and 165a of *the Penal Code*, it should be noted that in the recent analysis of the results of the progress made by Poland in the scope of the key and significant FATF Recommendations following the last assessment under the fourth round of mutual evaluations, the MONEYVAL Secretariat[374] concluded that they were to a broad extent consistent with the FATF Recommendations 1 and 35 and the FATF Special Recommendations I and II[375]

785. At the end of 2018, *Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law* was published (OJ L 284, 12.11.2018, p. 22). As indicated in the preamble: “Money laundering and the related financing of terrorism and organised crime remain significant problems at Union level, thus damaging the integrity, stability and reputation of the financial sector and threatening the internal market and the internal security of the Union. In order to tackle those problems and to complement and reinforce the application of Directive (EU) 2015/849 of the European Parliament and of the Council (2), this Directive aims to combat money laundering by means of criminal law, enabling more efficient and swifter cross-border cooperation between competent authorities.” Member States shall have time until 3 December 2020 to implement its provisions. The preliminary analysis shows that most of the regulations identified in it are reflected in national regulations.

786. In order to assess vulnerabilities in the area of money laundering and financing of terrorism, it is important to examine not only the regulations directly related to this subject, but also other regulations that may affect the effectiveness of the national anti-money laundering and counter-

[373] Meeting report - 56th plenary meeting Strasbourg, 3-6 July 2018, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism MONEYVAL, Strasbourg, 31 July 2018, p. 7, available at: https://www.coe.int/en/web/moneyval/activities/plenary-meetings.

[374] Analysis of 26 June 2018

[375] The fourth round of mutual evaluations verified the compliance with the FATF recommendations before their revision in 2012. At that time, 40 FATF Recommendations and 9 FATF Special Recommendations were in force. FATF Recommendations 1 and 2 addressed the scope of the money laundering crime whereas FATF Special Recommendations I and II addressed the ratification and implementation of UN instruments in the area of counteracting and combating the terrorist financing and criminalising terrorist financing.

terrorist financing system. In connection with the foregoing, it is worth noting that not all categories of obligated institutions, including those indicated in Article 2(1)(12), (16)-(18), (23)-(24) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* are subject to specialised, professional supervision. The situation is similar in the case of some of the entities indicated in Article 2(1)(11) of the aforementioned Act, in particular the so-called online bureaux de change offices. In the latter case, the change shall be caused by the regulations of the drafted *Act amending the Act - Foreign Exchange Law and certain other acts*. According to its assumptions, "non-cash currency exchange transactions performed by online bureaux de change offices and cash and non-cash currency exchange transactions" are to be subject to the provisions of *the Act of 19 August 2011 on payment services.*[376]

787. Another problem is the issue of the existence in the Polish legal order of bearer shares, which *in fact* make it impossible to identify the owners of such shares and which are not traded on the regulated market or have not been introduced into the alternative trading system[377] First of all, in order to resolve this problem, the Ministry of Justice prepared a draft *Act amending the Act - Commercial Companies Code and certain other acts* (on 13 June 2019 it was sent to the Sejm)[378] It provides for the introduction of obligatory dematerialisation of shares in joint-stock companies and limited joint-stock partnerships, which will be connected with identification of their holders.

7.2. VULNERABILITY OF THE ECONOMY

788. There are relatively few types of products and services offered in Poland that can directly facilitate quick and anonymous transactions.

789. In its transnational risk assessment of money laundering and financing of terrorism, the European Commission highlighted the relatively high level of vulnerability associated with the use of anonymous electronic money for money laundering (level 2/3 on a four-level scale) and for financing of terrorism (level 3/4 on a four-level scale). At the same time, as measures to mitigate this risk, it proposed to take legislative action to reduce the maximum limits for the failure to apply customer due diligence measures to e-money payment instruments, including prepaid cards.[379] These proposals are reflected in the provisions of Directive 2018/843. As indicated in subparagraph 5.3.1. of this report, the issuance of anonymous prepaid cards in Poland was limited in Article 38 of *the Act of 1 March 2018 on on counteracting money laundering and financing of terrorism*, more strictly than in Directive 2015/849. The maximum

---

[376] https://bip.kprm.gov.pl/kpr/form/r18139195608452,Projekt-ustawy-o-zmianie-ustawy-Prawo-dewizowe-oraz-niektorych-innych-ustaw.html, date of reading 28 June 2019

[377] In the case of bearer shares which are traded on a regulated market or have been introduced to an alternative trading system, they are dematerialised. Pursuant to Article 7(1) of *the Act on trading in financial instruments of 29 July 2005, "*the rights from dematerialised securities arise when they are recorded for the first time on a securities account and are vested in the person being the holder of that account". Pursuant to the provisions of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing* concerning the application of customer due diligence measures, holders of securities accounts must be identified and their identity verified (Article 34(1)(1) in conjunction with Article 35(1)(1)(2) and Article 36(1) of the aforementioned Act).

[378] https://legislacja.rcl.gov.pl/projekt/12294656/katalog/12410412#12410412, date of reading 28 June 2019

[379] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 66-67 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

limits indicated in that statutory provision are even lower than those indicated in Article 1(7) of Directive 2018/843 (with the exception of one concerning the situation of redeeming electronic money or withdrawing the value of electronic money in cash, which is equal to the limit defined in the aforementioned Directive). Currently, domestic banks do not issue prepaid cards which would represent electronic money instruments. On the other hand, in Poland it is possible to buy prepaid cards, including anonymous prepaid cards, offered by foreign institutions of electronic money acting on the basis of the European passport. However, it should be remembered that their countries of origin are also obliged to transpose EU regulations on anti-money laundering and counter-terrorist financing.

790. Since 13 July 2018, providers of virtual currency services have been subject to anti-money laundering and counter-terrorist financing regulations and are thus obliged to apply customer due diligence measures, including identification of customers and verification of their identity in situations provided for in the regulations.

791. The trade in cryptocurrencies is not explicitly regulated by the provisions of the Polish law[380], although there are certain positions and recommendations of public administration bodies concerning this issue. On 10 July 2014, the *Communication of the General Inspector of Financial Information on the hazards associated with virtual currencies* was published. The GIFI emphasised therein the alarming phenomenon of using virtual currency trading for criminal activities, including the money laundering practice.[381] On the other hand, on 7 July 2017, the Polish Financial Supervision Authority and the National Bank of Poland published a communication containing a warning notice related to cryptocurrency trading, indicating a number of risks, such as loss of funds, lack of BFG guarantee, general acceptability or potential fraud[382]

792. In the opinion of the KNF (PFSA), buying, holding and selling of virtual currencies by the entities supervised by the KNF (PFSA) is subject to high risk and does not ensure a stable and prudent management of the financial institution, in particular with regard to the risk of their use for money laundering and financing of terrorism. With regard to cryptocurrency exchanges, the KNF (PFSA) has adopted a warning approach, consisting, among others, in formulating supervisory expectations for financial institutions subject to its supervision, consisting in indicating the need to exercise particular prudence with regard to cooperation with entities operating cryptocurrency exchanges. For this reason, the KNF (PFSA) has also undertaken supervisory measures aimed at drawing the attention of the supervised entities to the need to

---

[380] An exception is *the Regulation of the Minister of Finance of 11 July 2018 on abandoning the collection of tax on civil law transactions on the contract of sale or exchange of virtual currency* (Journal of Laws, item 1348).

[381] Communication of the General Inspector of Financial Information on the hazards associated with virtual currencies, GIFI, 10 July 2014, available at: https://mf-arch2.mf.gov.pl/ministerstwo-finansow/dzialalnosc/GIFI/komunikaty/-/asset_publisher/8KnM/content/komunikat-generalnego-inspektora-informacji-finansowej-w-sprawie-niebezpieczenstw-zwiazanych-z-walutami-wirtualnymi?redirect=https%3A%2F%2Fmf-arch2.mf.gov.pl%2Fministerstwofinansow%2Fdzialalnosc%2FGIFI%2Fkomunikaty%3Fp_p_id%3D101_INSTANCE_8KnM%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn2%26p_p_col_count%3D1%26_101_INSTANCE_8KnM_advancedSearch%3Dfalse%26_101_INSTANCE_8KnM_keywords%3D%26_101_INSTANCE_8KnM_delta%3D5%26_101_INSTANCE_8KnM_cur%3D4%26_101_INSTANCE_8KnM_andOperator%3Dtrue#p_p_id_101_INSTANCE_8KnM_.

[382] Communication of the National Bank of Poland and the Polish Financial Supervision Authority on virtual "currencies", Warsaw, 7 July 2017, available at: https://www.nbp.pl/aktualnosci/wiadomosci_2017/komunikat-waluty-wirtualne.pdf.

terminate contracts with clients dealing in virtual currency or to refrain from establishing business relationships with clients in cases where it is not possible to apply customer due diligence measures, among others, to determine the source of origin of property values.

793. In November 2017, due to the growing problem associated with the cryptocurrency trading, the KNF (PFSA) sent a request to commercial banks, affiliating banks, cooperative banks and branches of credit institutions to provide information on accounts opened by the above institutions for cryptocurrency exchanges. The information provided by banks implied that the accounts for the aforementioned entities were maintained by both commercial banks and cooperative banks. Further analytical activities of the KNF (PFSA) caused these institutions to terminate their relations with such entities and declare to undertake measures resulting in refusing to enter into relationships with the so-called cryptocurrency exchanges in the future.

794. As a result of the process related to the termination of accounts by banks to the entities running cryptocurrency exchanges, a clear intensification of activities on the part of the above mentioned entities aimed at establishing cooperation with the DPI was observed. In the course of its analytical work, the KNF (PFSA) identified the risk of using the activities of domestic payment institutions for money laundering and financing of terrorism. The risk in question is particularly high in the situation of the aforementioned cooperation between the DPI and cryptocurrency exchanges.

795. With this in mind, in 2018 the KNF (PFSA) sent a letter to DPIs to determine whether they established and whether they maintain relationships with entities involved in virtual currency trading. Moreover, during the KNF (PFSA) inspection, significant risks were identified in the DPIs which are related to the maintenance of business relationships with cryptocurrency exchanges (e.g. in relation to customers for whom the entities operating cryptocurrency exchanges provide services through the network of accounts of the *collect* type[383] made available by the DPIs). As a rule, the DPIs do not have knowledge about customers who use the *collect* type accounts, thus not being able to determine where the clients of the entity running the cryptocurrency exchanges hold cryptocurrency and where the funds for their purchase come from. It should be also pointed out that services and products offered through entities operating cryptocurrency exchanges foster the anonymity.

796. According to the KNF (PFSA) communication of 6 June 2018[384] pursuing the activity in the territory of the Republic of Poland in the form of a cryptocurrency exchange or bureaux de change as well as trading in cryptocurrency, is not prohibited and is therefore legal. However, at the same time the KNF (PFSA) reminded that as of 13 July 2018 entities operating in the scope of cryptocurrency exchange or bureaux de change became obligated institutions within

[383] Information about this type of service can be found in subparagraph 5.3.1 in the description of threats in the banking area. It is also worth noting, that in Article 43(2)(6) of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*, the threat associated with the possibility of using this type of service for money laundering or financing of terrorism is emphasised, indicating that a higher risk in this area may be demonstrated by "the use by the customer of services or products conducive to anonymity or making its identification difficult, including the service consisting in creating additional account numbers marked in accordance with the regulations issued under Article 68(3) and (4) of the Act of 29 August 1997. - Banking Law and Article 4a(5) of the Act of 19 August 2011 on payment services, linked to the account held, for the purpose of making them available to other entities to identify payments or the parties ordering of these payments".
[384] Communication on the operation of cryptocurrency exchange or bureaux de change, UKNF (PFSA office), 6 June 2018, available at: https://www.knf.gov.pl/o_nas/komunikaty?articleId=61994_id=18.

the meaning of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*.

797. In the above mentioned communication, the UKNF (PFSA office) also indicated that carrying out this activity may involve the performance of activities covered by the relevant regulations governing the activity of entities on the financial market and, consequently, the obligation to obtain the relevant permits from the KNF (PFSA), e.g. a permit to perform payment services with respect to the maintenance of payment accounts (so-called virtual purses) and the execution of payment transactions specified in *the Act of 19 August 2011 on payment services.* In the period 2018-2019, the Polish Financial Supervision Authority identified a problem concerning cryptocurrency trading platforms involving conducting activities in the scope of payment services without the KNF (PFSA) licence - notifications were filed about a suspicion of committing a crime of activity against the regulations governing the financial market against 8 entities.[385]

798. It is also worth noting that a considerable part of entities offering virtual currency services, offering, among others, their services in Polish, is registered outside Poland, including outside the EU. For this reason, they are not committed to fulfil their obligations under *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* and sometimes they are not bound by the legislation of the country of registration to identify customers and verify their identity. In addition, P2P transactions are also carried out without any intermediation, which makes it easier to conceal the identity of the persons executing the transactions.[386]

799. Similarly to trading in cryptocurrency, crowdfunding does not have its own legal regulations. In its transnational risk assessment of money laundering and financing of terrorism, the European Commission highlighted the relatively high level of vulnerability in this area, both with respect to money laundering and to financing of terrorism (level 3 on a four-level scale).[387] This assessment is primarily justified by the lack of uniform, common regulations on anti-money laundering and counter-terrorist financing obligations relating to crowdfunding (only some EU Member States have introduced them). Operators providing services in this area also do not generally fall under the relevant controls. In addition, doubts have been raised as to whether these entities are sufficiently aware of the risks of financing of terrorism.

[385] Based on information from: https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne, date of reading 28 June 2019

[386] At the meeting of the FATF Policy Development Group (FATF) on 14-15 January 2019 among others, the vulnerabilities related to the risk of using virtual assets were indicated (defined as a concept broader than virtual currencies, also referring to any situation associated with the so-called "tokenisation" of other assets and their use within *blockchain* or other digital P2P formats and the possibility of using virtual assets both for payment settlement and investment purposes), i.e. the lack of a consistent global supervision of the anti-money laundering and counter-terrorist financing of entities providing virtual asset services, the lack of unification of legal regulations concerning the functioning of these entities in different jurisdictions as well as the application of standards for exchange transactions between individual virtual assets different from those relating to the exchange between virtual assets and legal means of payment.

[387] Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26 June 2017, pp. 55-56 (Annex 1 – Risk analysis by products), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

800. Another type of services fostering maintaining the anonymity of service recipients are the services offered by informal money transfer systems, such as *Hawala*. Although there are no detailed data concerning the scale of their functioning on the territory of Poland, it should be noted that the growing number of foreigners from high-risk countries (where such systems are in place) staying in the territory of the Republic of Poland gives rise to a suspicion that their activity may be developed on the territory of our country.

801. The lack of physical contact between customers and obligated institutions while applying customer due diligence measures relating to customer identification and verification of the customer's identity is also conducive to concealing their true identity. The Act of 1 March 2018 on counteracting money laundering and financing of terrorism addresses the above issue by indicating in Article 43(2)(7) that a higher risk of money laundering and financing of terrorism may be demonstrated by, among others, by "establishing or maintaining of business relationships or performing an occasional transaction without a physical presence of the customer - where the associated increased risk of money laundering and financing of terrorism has not been otherwise mitigated, including, through the use of notified electronic identification means adequately to the average security level, referred to in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, p. 73), or the requirement to use a qualified electronic signature or a signature confirmed by the ePUAP trusted profile." This is in line with the contents of the Interpretative Note to FATF Recommendation no. 10 (concerning the application of customer due diligence measures) which indicates that one of the higher risk factors for money laundering and financing of terrorism involves "non-face-to-face business relationships or transactions".[388]

802. While performing customer identification and verification of the customer's identity without using the above-mentioned means of electronic identification, there is a high risk of overlooking the fact that the personal data presented by the customer are not his or her own data or are falsified. This is particularly possible if, for example, the obligated institution uses only scans or scans of documents sent by the customer, not certified as true copies by any trusted third party.[389]

803. Among others, due to this vulnerability to the risk of concealing the customer's identity, the authorities of some other countries have issued detailed recommendations on the application of customer due diligence measures.[390] On 5 June 2019, the UKNF (PFSA office) published its position concerning customer identification and verification of customer identity in banks and

[388] International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated in October 2018, p. 63, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[389] At the same time, it is worth paying attention to the possibility of criminals using for this purpose the so-called collector documents, of which more information is provided in subchapter 5.1.7.

[390] An example of this may be the Canadian FIU guidelines, which state, among others, that: "It is not acceptable to view photo identification online, through a video conference or through any virtual type of application; nor can you accept a copy or a digitally scanned image of the photo identification." (available at: http://www.fintrac.gc.ca/guidance-directives/client-clientele/Guide11/11-eng.asp, date of reading 11 June 2019). The German financial supervision authority, on the other hand, provided the specific guidance on identifying customers and verifying their identity by video-conferencing (available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html;jsessionid=99FE32BBFAFE4CF5FCF35E96CEB2EA7B.1_cid298, date of reading 11 June 2019).

branches of credit institutions based on the video-verification method.[391] It was emphasised therein that the principles indicated in the above mentioned position should be applied accordingly when offering the video-verification service also by other institutions supervised by the UKNF (PFSA office).

804. In August 2018, the GIFI issued the communication in which it presented recommendations in the scope of procedure in the case of identification of a customer of an obligated institution and verification of his/her identity in the absence of his/her physical presence. Although it underlines the fact that, in accordance with Article 33(4) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, "the extent to which and the level of detail used by the obligated institution to apply customer due diligence measures to its customer shall depend on the risk identified and assessed by the obligated institution"[392], nevertheless, as a result of the doubts raised as to the application of the practices set out therein, in particular when simultaneous factors occur indicating a lower risk of money laundering and financing of terrorism, the next GIFI Communication was published in April 2019. It states that "The interpretation of the above mentioned provision [i.e. Article 43(2)(7) of the above mentioned Act] leads to the conclusion that the fact that the customer is not physically present when a business relationship is established or when an occasional transaction is carried out does not automatically indicate that there is a higher risk of money laundering and financing of terrorism, but can only indicate that such a risk exists. However, it is always the responsibility of the obligated institution to determine whether there is a higher risk of money laundering or financing of terrorism in a particular case, which recognises the risk of money laundering and financing of terrorism associated with the business relationship or occasional transaction in question and assesses the level of the risk recognised (Article 33 of the Act)."[393]

805. In the aforementioned FATF Interpretative Note to FATF Recommendation No. 10 it was also indicated that anonymous transactions, including cash transactions, may create a higher risk factor for money laundering and financing of terrorism.[394]

---

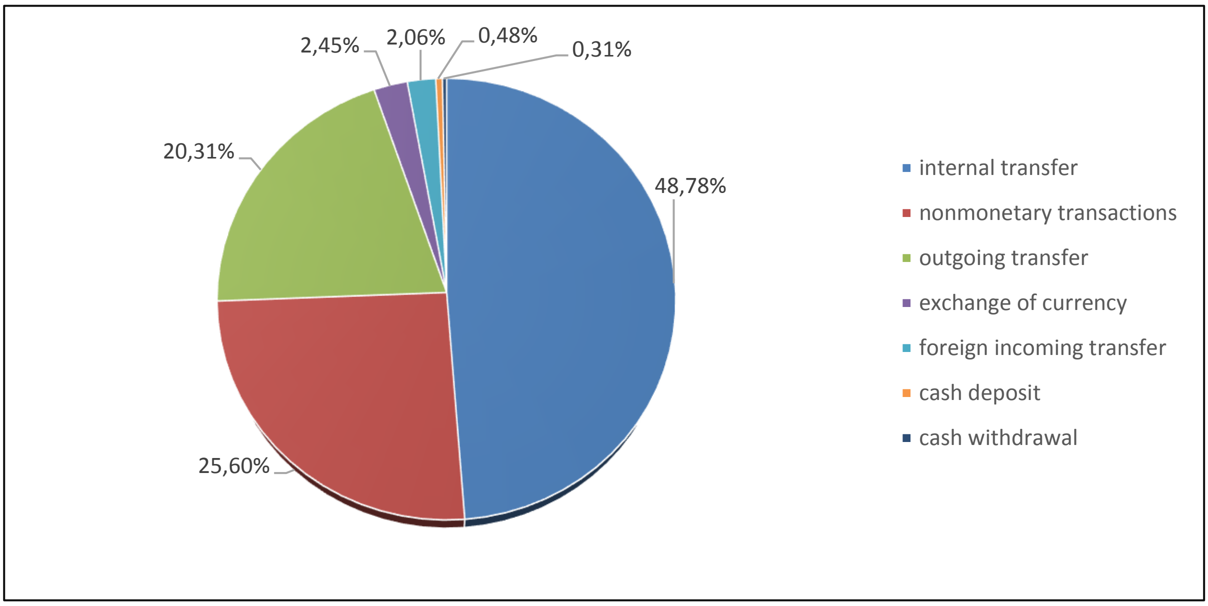
[391] The position of the UKNF (PFSA office) concerning the identification of the customer and verification of the customer's identity in banks and branches of credit institutions based on the video-verification method, UKNF (PFSA office), 5 June 2019, available at: https://www.knf.gov.pl/o_nas/komunikaty?articleId=66067&p_id=18.

[392] Guidelines of the General Inspector of Financial Information on identification of the customer of the obligated institution and verification of his identity in the absence of his physical presence, GIFI, 22 August 2018, available at: https://mf-arch2.mf.gov.pl/ministerstwo-finansow/dzialalnosc/GIFI/komunikaty.

[393] Communication No. 4 concerning the correction of the Communication of the General Inspector of Financial Information of 22 August 2018 on the identification of the customer of the obligated institution and verification of his identity, GIFI, 18 April 2019, available at: https://www.gov.pl/web/finanse/komunikaty-GIFI.

[394] International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated in October 2018, p. 63, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

Figure No. 16 - Information on the percentage share of the total value of transactions (converted into PLN) belonging to particular categories of transactions in the total value of all transactions sent to the GIFI in 2018.



806. The analysis of above-threshold transactions shows that out of approximately 35.97 million transactions submitted to the GIFI databases in 2018, transactions classified by obligated institutions to make cash payments or withdrawals made approximately 6.26%[395]. In 2017, it was about 6.72%, and in 2016 such transactions accounted for about 7.55%[396]

807. The share of the value of transactions classified by obligated institutions as cash deposits or withdrawals in the total value of all above-threshold transactions was relatively low. In 2018, it amounted to over 0.79% of the value of all above-threshold transactions sent to the GIFI at that time. The above data confirm the conclusions of the questionnaire and diary surveys mentioned in subchapter 5.3.2., conducted by the NBP in 2016, which indicate that although cash remains a commonly used means of payment, it is most popular for transactions with relatively low values[397]

808. It is worth mentioning that pursuant to Article 19 of *the Act of 6 March 2018 - Entrepreneur Law*, making or accepting payments related to their business activity should be performed via the entrepreneur's payment account, in each case when another entrepreneur is a party to the transaction from which the payment results and the single value of the transaction (regardless of the number of payments resulting from it) exceeds PLN 15,000 or the equivalent of this

[395] The share was calculated by categories of transactions, which were defined in item E of Annex No. 2 - "Structure of electronic recording", attached to *the Ordinance of the Minister of Finance of 21 September 2001 on determination of the sample register of transactions, the method of its maintenance and the mode of submitting the data from the register to the General Inspector of Financial Information* (Journal of Laws No. 113, item 1210, as amended).

[396] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, Warsaw 2019, p. 30.

[397] Arkadiusz Manikowski, Reasons for frequent cash selection by Poles - analysis of the results of the 2016 survey and diary survey, NBP 2017, p. 3-4, available at: https://www.nbp.pl/badania/seminaria/13xii2017.pdf

amount. Although the legislation does not provide for sanctions for non-compliance with this requirement, it is likely to have a significant impact on a limited number of cash transactions above this threshold.

809. Funds can be transferred in different ways. The most popular is the use of intermediary banks, followed by other financial institutions (SKOK or DPI and OPS). Banks represent the category of obligated institutions from which the greatest amount of information on suspicious transactions and activities reported to the GIFI originates.

810. In the case of descriptive reports of suspicious transactions and activities submitted in 2017, almost 94.9% came from banks and branches of credit institutions. Other obligated institutions operating on the financial market submitted over 2.8% of the descriptive notifications. Non-financial obligated institutions provided about 2.3% of the descriptive notifications.

Table no. 23 – Distribution of descriptive notifications from obligated institutions by type of obligated institution[398]

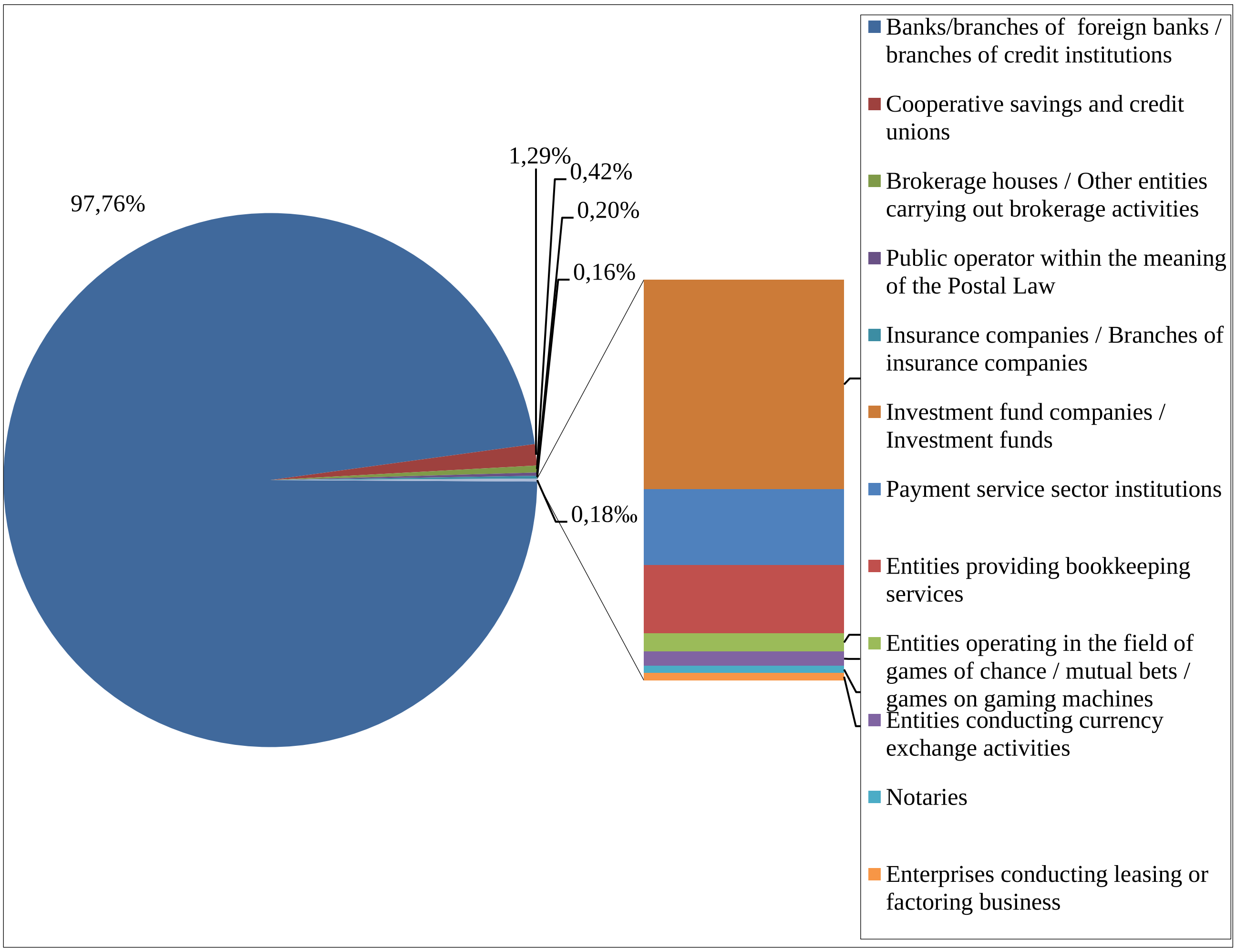
Type of institution	Number of descriptive notifications	Percentage share
Banks/ branches of foreign banks/ branches of credit institutions	3,104	94.87%
Brokerage houses / other entities carrying out brokerage activities	16	0.49%
Cooperative Savings and Credit Unions	44	1.34%
Insurance companies / branches of insurance companies	4	0.12%
Tax advisers, auditors and accountants	12	0.37%
Civil law notaries, legal counsels and attorneys	20	0.61%
Enterprises conducting leasing or factoring business	9	0.28%
Other entrepreneurs receiving payments in cash >=EUR 15,000	43	1.31%
Entities pursuing activity in the scope of currency exchange	1	0.03%
Institutions of the sector of payment services	19	0.58%
Total:	**3,272**	**100.00%**

811. A similar distribution was found in the case of information on single transactions(i.e. STR), the circumstances of which may indicate a link with the commissioning of a money laundering or financing of terrorism offence. Almost 97.8% of this information in 2017 came from banks and branches of credit institutions and about 2.0% from other obligated institutions operating on the financial market. A relatively small share of information (more than 0.2%) was reported by non-financial obligated institutions.

812. Such a large amount of information from banks and branches of credit institutions indicates that the financial flow channels within their competence are relatively well monitored.

[398]Based on information from: Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2017, Warsaw 2018, p. 10.*

Figure No. 17 – Sources of the STRs in 2017[399]



813. Among above-threshold transactions submitted in 2018 the GIFI, approx. 12.50% were the transactions involving entities for which the obligated institution indicated the domicile outside the territory of Poland or the citizenship other than Polish and approx. 3.51% of transactions were classified by the obligated institutions as incoming from abroad.[400] There has been a slight increase compared to 2017 figures. Transactions involving entities for which the obligated institution has indicated a place of residence outside Poland or citizenship other than Polish, accounted for approx. 13.12% of all above-threshold transactions (in 2016, there were 11.46% of such transactions, including 3.40% of transactions classified by obligated institutions as incoming transfers from abroad)[401]

814. The analysis carried out in 2018 by the UKNF (PFSA office)[402] on the basis of data on transfers with a unit value of more than PLN 2 000, provided by supervised obligated institutions (without taking into account the SKOK data) shows that the total value of all outgoing foreign transfers from Poland in 2017 amounts approximately to PLN 1.49 trillion

[399]Ibidem, p. 11.
[400] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, Warsaw 2019, p. 30.
[401] Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2017,* Warsaw 2018, p. 15.
[402] The above analysis constitutes Annex 4 to this report.

while the total value of all foreign transfers incoming to Poland in 2017 amounts to approximately PLN 2.95 trillion.

815. In the case of foreign transfers outgoing from Poland, the highest amounts of money were transferred to Germany, the United Kingdom, Sweden and the Netherlands (about PLN 306.82 billion, about PLN 210.04 billion, about PLN 126.09 billion and about PLN 107.25 billion, respectively). The total value of outgoing transfers from Poland to these countries constituted approximately 50% of all outgoing transfers from Poland. The above mentioned countries were followed by the USA (about PLN 85.3 billion), followed by Finland, France, Italy and Denmark.

816. In terms of foreign transfers incoming to Poland, the highest amounts of money came from Germany, the USA, the United Kingdom, Sweden, Switzerland, Denmark, the Netherlands, France and Finland (respectively: about PLN 642.06 billion, about PLN 458.16 billion, about PLN 292.80 billion, about PLN 270.86 billion, about PLN 150.06 billion, about PLN 142.64 billion, about PLN 141.95 billion, about PLN 112.02 billion and about PLN 107.78 billion).

817. The data collected by the UKNF (PFSA office) for the purposes of the above analysis also show that the supervised obligated institutions kept accounts for about 615.18 thousand of non-residents in 2017 (the highest number - for Ukrainian entities - i.e. 319,915, followed by entities from Germany - 51,696, Belarus - 27,334, the UK - 24,851 and the USA - 16,345).

818. The analysis of data concerning incoming and outgoing transfers to and from Poland also took into account transfers from and to countries where ISIS operated, as well as neighbouring countries (excluding Israel).

819. Most of the money was transferred between Poland and Turkey, Lebanon and Saudi Arabia, as well as Jordan and Kuwait, which reflects trade with these countries. The above data indicate a relatively low percentage share of outgoing and incoming foreign transfers from Iraq and Syria in relation to the total value of outgoing and incoming foreign transfers to Poland in 2017.

Table no. 24 - Values of foreign transfers between Poland and the countries where the so-called Islamic State operated as well as neighbouring countries (excluding Israel), executed in 2017 (in PLN million)[403]

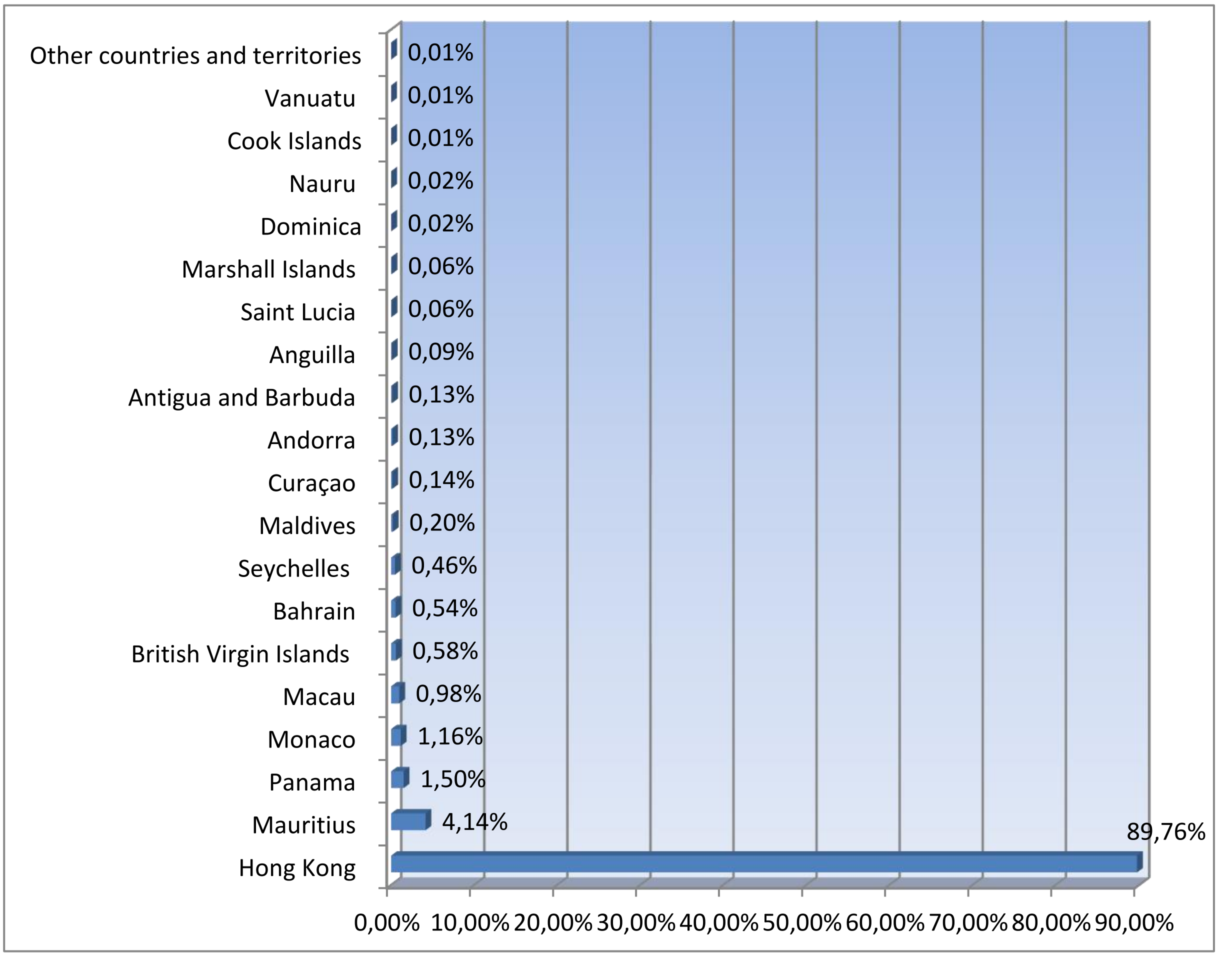
country	value of foreign transfers outgoing from Poland	value of foreign transfers incoming to Poland
Turkey	18,125.96	5,781.16
Lebanon	94.86	118.86
Saudi Arabia	86.82	411.81
Jordan	37.2	57.63
Kuwait	19.63	90.49
Iraq	5.95	15.02
Iran	0.41	38.8
Syria	0.03	0.32

820. Most of the money was transferred between Poland and Turkey, Lebanon and Saudi Arabia, as well as Jordan and Kuwait, which reflects trade with these countries. The above data indicate a relatively low percentage share of outgoing and incoming foreign transfers from Iraq

[403] Based on the data derived from Annex No. 4

and Syria in relation to the total value of outgoing and incoming foreign transfers to Poland in 2017.

Figure no. 18 - Share of the value of foreign transfers outgoing to particular countries and territories indicated in the Regulations of 17 May 2017 of the Minister of Development and Finance up to the total value of foreign transfers outgoing to these countries and territories[404]



821. The analysis of UKNF (PFSA office) also shows that in 2017 the total amount of approximately PLN 11.48 billion was sent from Poland to countries and territories which can be recognised as tax havens[405] (which represents approximately 0.8% of the value of all foreign transfers outgoing from Poland in the indicated period). The highest amount - about PLN 10.31 billion - was sent to Hong Kong. The above amount significantly exceeds the 2017 figures for

---

[404] Based on the data derived from Annex No. 4.

[405] Based on the lists indicated in the *Ordinance of the Minister of Development and Finance of 17 May 2017 on the definition of countries and territories applying harmful tax competition in the field of personal income tax* (Journal of Laws, item 998) and the *Ordinance of the Minister of Development and Finance of 17 May 2017 on the definition of countries and territories applying harmful tax competition in the field of corporate income tax* (Journal of Laws, item 997).

In 2019, the above-mentioned legal acts were replaced by new regulations: *the Ordinance of the Minister of Finance of 28 March 2019 on the definition of countries and territories applying harmful tax competition in the field of personal income tax* (Journal of Laws, item 599) and *the Ordinance of the Minister of Finance of 28 March 2019 on the definition of countries and territories applying harmful tax competition in the field of corporate income tax* (Journal of Laws, item 600).

Poland's trade in goods with Hong Kong. Such a high value of the transferred money may indicate not only a possible link with money laundering but also a desire to hide the actual owner of the transferred money or take advantage of tax optimisation.

822. The UKNF (PFSA office) also analysed data on outgoing transfers to countries and territories which in 2018 were indicated in the FATF documents as:

- countries and territories which have strategic deficiencies with whom the FATF cooperates due to the fact that they pose threat to the international financial system;
- with whom the FATF cooperates and monitors to verify progress in addressing identified shortcomings in the area of anti-money laundering and counter-terrorist financing (and which at the same time are called by the FATF for the rapid implementation of action plans within the proposed timeframe).

823. Of these jurisdictions, most of the money was transferred to Serbia, Pakistan, Bosnia and Herzegovina and Tunisia. Such a value of transactions with these countries is reflected in the recently revived mutual trade relations between Poland and these countries.

Table no. 25 - Value of outgoing foreign transfers in 2017 to countries and territories considered as high-risk areas and requiring constant monitoring in accordance with FATF recommendations (in PLN million)[406]

name of the country/ territory	value of transfers outgoing from Poland
Serbia	1,391.37
Pakistan	306.56
Bosnia and Herzegovina	283.16
Tunisia	139.89
Sri Lanka	57.61
Afghanistan	13.99
Laos	11.35
Uganda	8.05
Ethiopia	3.69
Trinidad and Tobago	1.94
Vanuatu	0.85
Yemen	0.11
North Korea	0.07
Guyana	0.04

824. The majority of entities which should - on the basis of an analysis of threats to money laundering or financing of terrorism - be subject to regulations governing the prevention of these crimes have been included in the catalogue of obligated institutions. Some entities which have been identified in the transnational risk assessment of money laundering and financing of terrorism and in the provisions of Directive 2018/843 should additionally be introduced into the above catalogue as separate categories, in particular:

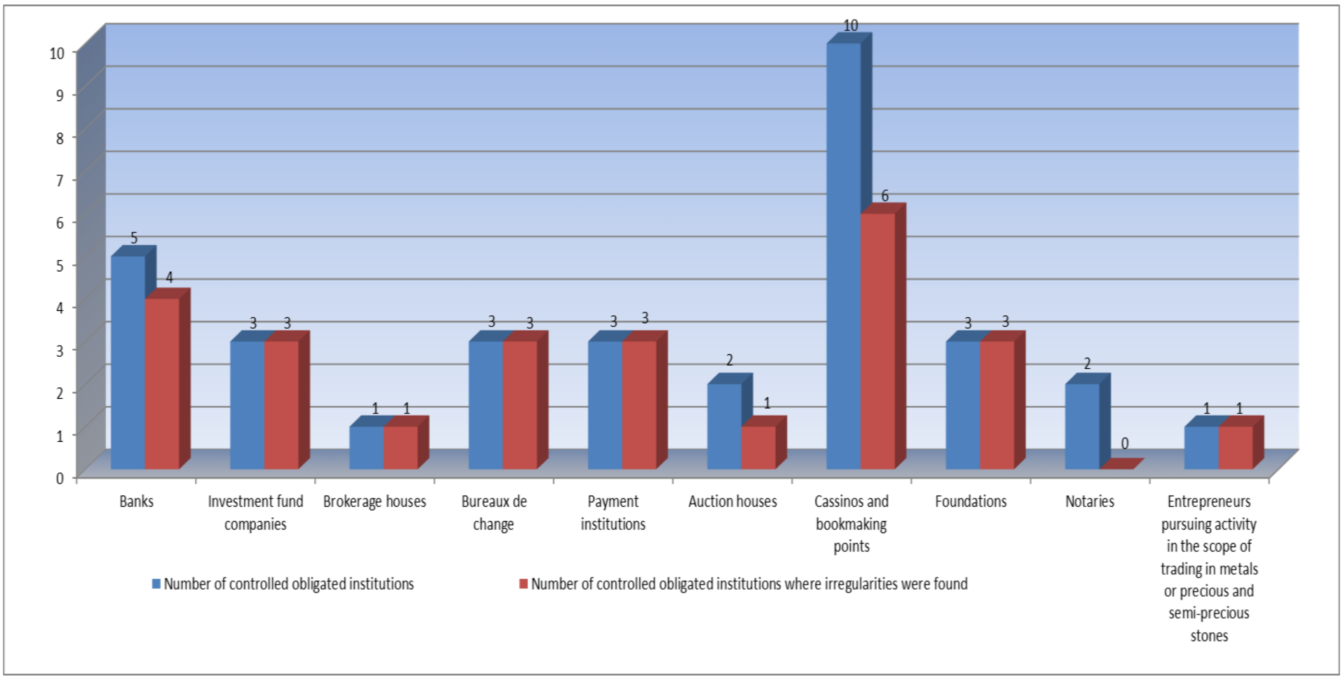
- entities offering crowdfunding services;
- persons trading in works of art or acting as intermediaries in the trade in works of art, including where such trade is conducted by art galleries and auction houses, if the value of the transaction or a series of related transactions is EUR 10,000 or more;

[406] Based on the data derived from Annex No. 4. The table does not include data concerning Iraq, Iran and Syria, which have already been presented before.

- persons storing works of art, trading in works of art or acting as intermediaries in the art trade, where such activity is carried out through *free ports*, if the value of the transaction or a series of related transactions is EUR 10,000 or more;
- any persons (not only statutory auditors, external accountants and tax advisers) who undertake to provide, directly or through other persons with whom they are linked, material assistance, support or advice on tax matters in the course of their main business or professional activities.

825. Inspections of the GIFI carried out in 2017 among 25 obligated institutions revealed irregularities in the implementation of obligations arising from the provisions of anti-money laundering and counter-terrorist financing legislation in 20 entities. On the other hand, the audits carried out by the GIFI in 2018 revealed weaknesses in the implementation of these obligations in 5 of the 8 institutions audited.

Figure no. 19 - Information on inspections carried out by the GIFI in obligated institutions in 2017-2018



826. The inspections carried out by the GIFI in 2018 revealed violations such as:

- the failure to adjust internal procedures to the provisions of the *Act of 16 November 2000 on counteracting money laundering and financing of terrorism*;
- lack of registration of transactions of the equivalent exceeding EUR 15,000, referred to in Article 8(1) of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism*;
- providing the GIFI with information related to transactions violating the time limit referred to in Article 12(2)(1) of the aforementioned Act;
- registration of transactions violating the time limit specified in § 2(2) of *Ordinance of 21 September 2001 of the Minister of Finance on determining the template of the Register of Transactions, the manner to keep the Register, and the mode to provide*

data from the Register to the General Inspector of Financial Information, hereinafter referred to as the Ordinance;

- failure to perform risk analysis in relation to a part of clients covered by the sample,
- failure to apply customer due diligence measures referred to in Article 8b(3) and Article 9e(2) of the aforementioned Act;
- failure to carry out an ongoing analysis of the transactions carried out during the period subject to inspection
- failure to document and file results of the current analysis of all transactions conducted, imposed by Article 8a of the aforementioned Act;
- failure to ensure participation of employees performing anti-money laundering and counter-terrorist financing duties in training programs in the scope of the Act, referred to in Article 10a(4) of the aforementioned Act.

827. Infringements in this scope, to the extent indicated above, were detected during inspections carried out in 2017 and in addition to these:

- irregularities in the scope of completing transaction cards;
- failure to take into account the principles indicated in §4(3) of the aforementioned Ordinance, through compromising the structure of the electronic record, defined in Annex no. 2 to the Ordinance;
- submission of a hard copy of data related to more than one transaction to the GIFI, which is not compliant with §7(1) of the Ordinance;
- assigning inappropriate risk category to a part of clients covered by the sample;
- the risk category was unknown to employees of the obligated institution branches;
- the notifications to the GIFI regarding transactions referred to in Article 16(1) and (17) of the Act were too general;
- failure to provide the GIFI with documents related to transactions referred to in Article 8(1) of the Act as well as missing the time limit for providing the GIFI with the documents concerning the transactions.

828. Based on the results of inspections carried out by the UKNF (PFSA office) in 2017 in relation to the fulfilment of its anti-money laundering and counter-terrorist financing obligations, it was found that the largest number of irregularities, in relation to the number of entities inspected, occurred in the sector of cooperative banks - on average, 10.30 irregularities per inspection with an average for all inspections of 7.58. However, no systemically significant irregularities were found in any of the sectors audited.

829. In 2018, within the performed inspections, the UKNF (PFSA office) focused primarily on how to determine the beneficial owner and the inspections of the payment institutions in particular included an element of training for agents by these authorities. In addition, the audits also focused on the provision of safe deposit box services by banks.[407] This was a direct result

[407] Report of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2018, Warsaw 2019, p. 72, available at: https://www.knf.gov.pl/publikacje_i_opracowania/sprawozdania.

of the recommendations issued by the European Commission on the areas identified as requiring specific research. All the inspections carried out by the UKNF (PFSA office) in these areas revealed irregularities and weaknesses. The largest number of these concerned the implementation of the obligation to assess risks and apply customer due diligence measures (this was mainly due to the fact that the checks carried out were focused on identifying the beneficial owner). Other areas where relatively many irregularities were identified included the organisation of the anti-money laundering and counter-terrorist financing process and the provision of information to the GIFI.[408]

830. In the case of inspections carried out by the NBP, the share of entrepreneurs conducting bureaux de change activity who were found to have irregularities in the implementation of obligations concerning counteracting money laundering and financing of terrorism was relatively small in relation to all the controlled entrepreneurs conducting bureaux de change activity, in 2018 it was 4.87%, in 2017. - 4.14%, and in 2016. - 4,96%.

831. Although the obligated institutions from most of the categories indicated in Article 2(1) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* are aware of the obligations imposed on them by the anti-money laundering and counter-terrorist financing regulations[409], attention should be paid to a relatively large number of irregularities found during inspections carried out by the GIFI and the UKNF (PFSA office). Moreover, it is worth noting the relatively low amount of information on transactions and suspicious activities that have so far been reported by categories of obligated institutions other than banks, in particular non-financial institutions.

832. Until the entry into force of the aforementioned Act, only pecuniary and penal sanctions were in force for non-compliance by the obligated institutions with the principles set out in the aforementioned regulations, with pecuniary sanctions being imposed exclusively by the GIFI.

833. In 2018 the GIFI carried out 49 administrative proceedings for the imposition of fines on the obligated institutions for failing to observe the provisions of the Act and in 2017 - 99.[410] As a result, the GIFI issued 120 decisions (85 in 2017 and 35 in 2018), in which it imposed fines in the total amount of PLN 1,490,900.

---

[408]Ibidem, p. 73.

[409] In the questionnaires distributed in the second half of 2017 by the GIF (filled in by 41 representatives of bodies authorized to control obligated institutions under the anti-money laundering and counter-terrorist financing regulations, mainly representing customs and tax control offices - 21, courts of appeal - 9, governors of provinces - 7, as well as the KNF (PFSA), the NBP and the National SKOK) about 61.0% of respondents assessed the effectiveness of activities of obligated institutions in the analysed area at a high or very high level (level 3 and 4 on a four-level scale). At the same time, in relation to the question concerning the level of awareness of employees of obligated institutions to take risks related to money laundering and terrorist financing, most respondents indicated its high or very high level (i.e. 3 and 4 on a four-level scale) among persons employed in domestic banks, branches of foreign banks and branches of credit institutions (level 4 indicated by 10 respondents), notaries (level 4 indicated by 13 respondents), entities operating in the field of gambling, betting and gaming machines (level 3 indicated by 13 respondents). None of the assessments in relation to the above question indicated level 1 (i.e. low awareness of the risk of money laundering and terrorist financing).

[410] Information Based on the data derived from: Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and financing of terrorism and the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2018, Warsaw 2019, pp. 47-49; Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism* in 2017, Warsaw 2018, pp. 33-34.

834. In connection with appeals lodged against GIFI decisions (including, in two cases against decisions issued before 2017), in 2017, the Minister of Development and Finance upheld 7 decisions of the GIFI, in 4 cases - waived the GIFI decisions in their entirety and adjudicated fines in lower amounts, in 1 case - waived the GIFI decision in its entirety and discontinued first instance proceedings in a part, and in 1 case - discontinued appeal proceedings. On the other hand, in 2018, the Minister of Finance upheld 3 decisions of the GIFI; in 2 cases - waived the decision of the GIFI in its entirety and adjudicated fines in lower amounts and in subsequent 2 cases - waived the decision of the GIFI in its entirety and discontinued proceedings entirely.[411]

835. Moreover, in 2017 The GIFI submitted 18 notifications to the Prosecutor's Office on committing crimes which are exhaustive in terms of acts specified in Article 35 of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism*, and in 2018 - 3 notifications under the above provision. In addition, also in 2017, the UKNF (PFSA office) sent one notification to the public prosecutor's office under the provisions of the aforementioned Act.

7.3. VULNERABILITY IN THE SCOPE OF ACTIVITIES OF PUBLIC ADMINISTRATION AUTHORITIES AND UNITS

This subchapter presents general information on the activities of public administration authorities and units, broken down into supervision authorities, law enforcement agencies, financial intelligence units and judicial authorities, affecting the assessment of vulnerability to money laundering and financing of terrorism. Annex 5, on the other hand, provides a detailed description of selected authorities and units.

7.3.1. Activities of supervision authorities

836. In accordance with the provisions of the currently effective *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, besides the GIFI, control activities in obligated institutions in the scope of compliance with the provisions of the above-mentioned Act and other acts of law, are also carried out by:

- President of the NBP (in relation to entities pursuing bureaux de change activities);
- KNF (PFSA) (in relation to obligated institutions supervised by it);
- National Cooperative Savings and Credit Union (in relation to cooperative savings and credit unions);
- presidents of courts of appeals (in relation to notaries public);
- heads of customs and tax control offices (with respect to all obligated institutions);

[411] In 2017, 5 complaints against the decisions of the Minister of Development and Finance were lodged with the Regional Administrative Court in Warsaw (WSA). In 2017, the WSA dismissed entirely 5 complaints against the decisions of the Minister of Development and Finance; 2 complaints were filed with the Supreme Administrative Court (NSA). On the other hand, in 2018, 2 complaints against the decisions of the Minister of Finance were lodged with the WSA (including 1 complaint against the administrative proceedings conducted in 2017). In 2018, the WSA dismissed entirely 1 complaint against the decision of the Minister of Finance; in the second case the procedure was pending. At that time 2 cassation complaints were lodged with the NSA. In 2018, the NSA dismissed entirely 2 cassation appeals (including 1 cassation appeal lodged in 2017). In 2018, in 2 cases the procedure before the NSA were pending (in 1 case - following the cassation appeal lodged in 2017).

- ministers or governors of districts – in relation to foundations;
- governors of provinces or governors of districts – in relation to associations.

837. Answering one of the questions included in the questionnaires distributed by the GIFI in the second half of 2017, the overwhelming majority of respondents, representing supervision authorities[412] indicated that the financial and equipment resources needed to carry out inspections of obligated institutions, including the compliance with anti-money laundering and counter-terrorist financing regulations, are sufficient (about 68.3% of respondents and about 65.9% of respondents respectively). In the case of human resources, however, although a part of respondents described human resources as adequate (about 48.8% of the respondents), about 41.5% of the respondents indicated that they were not satisfactory. Furthermore, in the justification, apart from an insufficient, small number of controllers, the lack of specialised training on anti-money laundering and counter-terrorist financing as well as guidelines, recommendations and motivations was also mentioned.

838. The Financial Information Department of the Ministry of Finance, which supports the GIFI in carrying out its statutory tasks, is responsible, inter alia, for carrying out inspections of obligated institutions and administrative proceedings on the basis of anti-money laundering and counter-terrorist financing regulations. As in the case of the replies to the above-mentioned questionnaire, the financial and equipment resources needed to control the obligated institutions by the Department controllers acting on behalf of the GIFI, should be determined as sufficient. On the other hand, in terms of human resources, within the preparation of the 2017 Regulatory Impact Assessment for the then draft *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, among others, the need to expand the composition of the Department's unit dealing with these issues by 4 additional persons was indicated[413].

839. In the years 2017-2018, a relatively large number of inspections were carried out on the compliance of obligated institutions with their obligations arising from anti-money laundering and counter-terrorist financing legislation.

840. Although a relative decrease in the number of inspections can be observed, it is worth remembering that on 13 July 2018, *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* came into force, which changed the scope of implementation of anti-money laundering and counter-terrorist financing tasks by obligated institutions, affecting the number of inspections.

Table No 26 - Number of inspections carried out in the obligated institutions in 2017-2018 by individual categories of authorities[414]

Authority	**2017**	**2018**
NBP	656	402

[412] Filled in by 41 representatives of bodies entitled to control obligated institutions under anti-money laundering and counter-terrorist financing regulations, mainly representing customs and tax control offices - 21, courts of appeal - 9, governors of provinces - 7 as well as the KNF (PFSA), the NBP and the National SKOK.
[413] At the turn of 2017 and 2018 the above-mentioned unit consisted of 8 people, currently, i.e. as of 31 May 2019 - 11.
[414] Information Based on the data derived from: Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and financing of terrorism and the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2018, Warsaw 2019, pp. 46-48; Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism* in 2017, Warsaw 2018, pp. 31-33.

National Cooperative Savings and Credit Union	9	12
KNF (PFSA)[415]	50	37
Presidents of courts of appeal	171	135
heads of customs offices, customs and tax control offices, tax control offices	53	19
GIFI	25	8
governors of provinces and districts	-	15

841. As indicated in subchapter 7.2., in the years 2017-2018, on the basis of the results of inspections carried out, the GIFI imposed fines, as well as sent notifications to the prosecutor's office on suspicion of committing an offence in connection with the failure of obligated institutions to comply with the obligations resulting from anti-money laundering and counter-terrorist financing regulations (in one case such notification was sent by the UKNF (PFSA office)).

842. While imposing fines, the GIFI relied not only on the findings of inspections carried out by the staff of the Financial Information Department of the Ministry of Finance, but also on the results of inspections undertaken by other authorities which provided regular information thereon.

843. It is worth noting that in the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, substantial emphasis was placed on the cooperation between the GIFI and other authorities in the scope of controlling the obligated institutions. Among others, it was indicated that the GIFI coordinates inspections performed by other authorities. As part of this coordination, it develops and makes available, by 15 November each year, information on areas and sectors particularly vulnerable to the risk of money laundering or financing of terrorism, and may provide the aforementioned authorities with guidelines concerning the control of the compliance with the provisions of the aforementioned Act (Article 132 of the above-mentioned Act). Moreover, the GIFI has a possibility to request the above-mentioned authorities to carry out ad-hoc inspections in obligated institutions. On the other hand, the aforementioned authorities are bound to submit to the GIFI annual inspection plans with justification - however, not later than by 31 December of the year preceding the inspection as well as updates of the plans, within 14 days from the date of their preparation, notification of the intention to carry out an ad hoc inspection with justification - not later than on the date of commencement of the inspection, unless the inspection results from the updated inspection plan, as well as information about the findings of the inspection, within 14 days from the date of its completion or issuance of post-control recommendations or taking a decision on withdrawal from their issuance (Article 131(4)-(5) of the aforementioned Act).

844. The GIFI, like the UKNF (PFSA office), cooperates closely with its foreign counterparts, both in the framework of bilateral and multilateral contacts (on the fora of various international organisations, including the European Union, the Egmont Group and the MONEYVAL Committee). In the case of the GIFI, this cooperation consists, inter alia, in the exchange of experience in the entire spectrum of activities of financial intelligence units.

845. The UKNF (PFSA office) cooperates with foreign financial market supervision authorities (under the signed cooperation and information exchange agreements with supervision

[415] Data adjusted on the basis of information on control activities carried out derived from the Report on activities of the Polish Financial Supervision Authority in 2017, Warsaw 2018, p. 69; Report on activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2018, Warsaw 2019, p. 73, available at: https://www.knf.gov.pl/publikacje_i_opracowania/sprawozdania.

authorities from 49 countries[416]). Moreover, the UKNF (PFSA office) cooperates and exchanges information with 128 foreign counterparts - members of the International Organization of Securities Commissions (IOSCO) and with the ESMA. In addition, the UKNF (PFSA office) had agreements concluded with 3 jurisdictions in the scope of cooperation within *FinTech*.

7.3.2. Activities of the Financial Intelligence Unit

846. Article 32 of Directive 2015/849 requires each EU Member State to have a financial intelligence unit (FIU) in place to counteract, detect and effectively combat money laundering and financing of terrorism incidents. This objective shall be achieved, in particular, by receiving and analysing suspicious transaction reports and other information on money laundering, related predicate offences or financing of terrorism and by communicating the results of analyses and any other relevant information to the competent authorities where grounds for suspecting such offences exist. In addition, the FIU must be equipped with the powers to take immediate action, directly or indirectly, where there is a suspicion that the transaction is related to money laundering or financing of terrorism and to suspend or withhold the consent to continue the transaction under processing in order to analyse the transaction, confirm the suspicions and disclose the results of the analysis to the competent authorities (also at the request of the FIU from another EU Member State).

847. The financial intelligence unit must be independent and operationally autonomous, i.e. have the powers and capacity to exercise its functions freely, including the ability to take autonomous decisions on the analysis, request and dissemination of specific information. It is the State responsibility to make adequate financial, human and technical resources available to it to carry out its tasks.

848. The financial intelligence unit must be able to obtain additional information from the obligated institutions and have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires for the due performance of its tasks. In addition, it must be able to provide information on request of competent authorities where the basis for those requests relates to money laundering, related predicate offences or financing of terrorism. On the other hand, the competent authorities are required to provide feedback to the financial intelligence unit on the use of the information received from it.

849. Article 53 of Directive 2015/849 requires the financial intelligence unit to exchange information with financial intelligence units from other EU Member States (on its own initiative or on request). This exchange should concern any information which might be relevant in the context of the processing or analysis of information by the particular financial intelligence unit and related to money laundering or financing of terrorism and the natural or legal person involved in those activities (even if at the time the information is exchanged, there is no specific type of predicate offence to which the information might relate).

850. In the case of Poland, the function of the financial intelligence unit is exercised by the GIFI jointly with the Financial Information Department of the Ministry of Finance, supporting it in carrying out its statutory tasks (described in chapter 4.3.1.).

---

[416] According to the data for June 2018.

851. However, it should be stressed that the scope of the GIFI's tasks is broader than those assigned to the financial intelligence units of EU Member States under Directive 2015/849. In particular, the GIFI:

- exercises the control of compliance of the obligated institutions with the obligations in the scope of counteracting money laundering and financing of terrorism;
- coordinates such controls exercised by other authorities;
- imposes administrative penalties on institutions for the failure to comply with anti-money laundering and counter-terrorist financing legislation;
- develops and updates the national assessment of the risk of money laundering and financing of terrorism;
- develops draft strategy for counteracting money laundering and financing of terrorism;
- implements tasks in the scope of special restrictive measures, including issuing decisions concerning entering in the list of persons and entities towards which special restrictive measures are used or concerning their striking-off the list as well as keeps the aforementioned list.

852. In addition, the GIFI is the administrator of the ICT system used to carry out its tasks. It is currently undergoing reconstruction, mainly in connection with its adjustment to the requirements arising from *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*.

853. The above tasks (including those related to the administration of the aforementioned system) are performed by the Financial Information Department of the Ministry of Finance. Its activities are financed from the budget of the Ministry of Finance.

854. The GIFI also strives to strengthen the knowledge of obligated institutions and cooperating units in the area of anti-money laundering and counter-terrorist financing and the awareness of risks connected with it, inter alia, by issuing announcements and publishing information in the section dedicated to the Ministry of Finance (under the tab related to the GIFI activities) on the website www.gov.pl. Moreover, in February 2019, the GIFI launched a new edition of the e-learning course entitled "Counteracting money laundering and financing of terrorism" (referring in particular to the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*), addressed to employees of obligated institutions as well as to cooperating units.

855. Over the last few years, the number of employees of the Financial Information Department of the Ministry of Finance has been slowly increasing, reaching 75 at the end of May 2019[417]. The assessment of the possibility of performing the tasks imposed on the above mentioned unit, in particular the obligations which are currently based on *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, shows that more resources are needed. For this reason, the Regulatory Impact Assessment for the aforementioned act of law

[417] At the end of 2017, 64 people were employed.

indicated the need to employ 24 new employees[418], some of whom have already been recruited.[419]

856. In general, employees of the above-mentioned Department are very well aware of the risks in the area of money laundering and financing of terrorism. Moreover, they also participate in training activities related to this issue organised by both the GIFI and other public administration bodies (information about these training activities is presented in the reports on the annual activity of the GIFI). Nevertheless, there is a need for a specific, separate programme of periodic training, especially for employees of the analytical division. Currently, newly hired analysts undergo practical training in the unit dealing with the initial analysis of information about suspicious transactions and activities.

857. According to the annual reports of the GIFI on the implementation of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism*, in 2016-2017, the GIFI initiated - on the basis of the information obtained - 2,506 and 2,567 analytical proceedings, respectively. At the same time, it should be noted that their number has increased in subsequent years. In 2016, this increase - compared to data for 2015 - reached about 12.4%, and in 2017 - in relation to the previous year - about 2.4%. However, the data for 2018 show that the number of analytical proceedings amounted to 2,160, i.e. approx. 15.9% less than in 2017. However, it should be remembered that the number of conducted analytical proceedings is not directly correlated with the number of reports on suspicious activities, in particular transactions, received from obligated institutions or cooperating entities. Several to several dozen (and sometimes even more) pieces of this type of information may be analysed within a single analytical procedure[420]

858. As part of its analytical proceedings, on the basis of anti-money laundering and counter-terrorist financing legislation, the GIFI addresses cooperating units[421] and obligated institutions in order to collect additional information necessary to confirm or deny the initial assessment relating to suspected money laundering or financing of terrorism. Moreover, the GIFI has a direct or indirect access to most of the databases maintained by public administration entities. Exceptions apply mainly to internal databases of the services and the STIR.

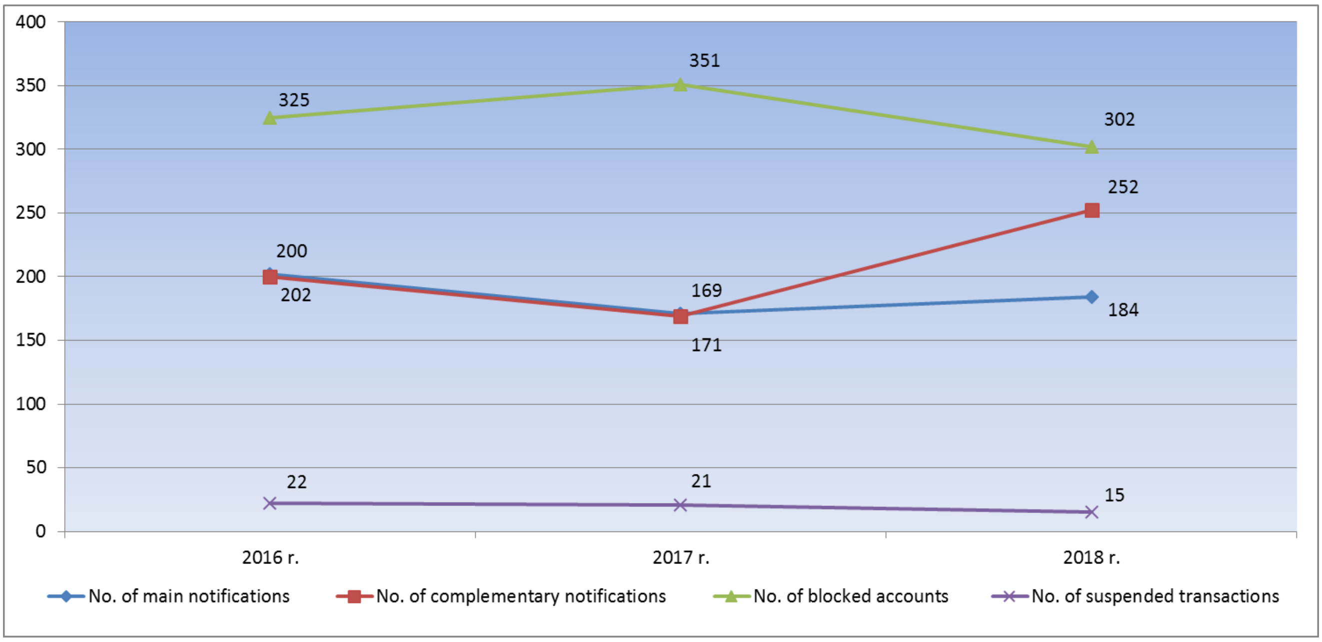
Figure no. 20 – Specification concerning the number of notifications submitted to prosecutor's offices, blocked accounts and suspended transactions in 2016-2018

[418] The aforementioned Regulatory Impact Assessment also indicates the need to hire 9 employees at the Ministry of Finance to perform tasks related to the functioning of the Central Register of the Beneficial Owners.

[419] The question whether the target number of the Department's employees will be sufficient can be answered only after the full implementation of the provisions of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing* (including the provisions of implementing regulations specified in this Act), as well as completion of the currently implemented activities both in terms of employment and changes in the GIFI ICT system.

[420] The decrease in the number of analytical proceedings in 2018 could have also been influenced by the amendments in anti-money laundering and counter-terrorist financing regulations and in their implementation.

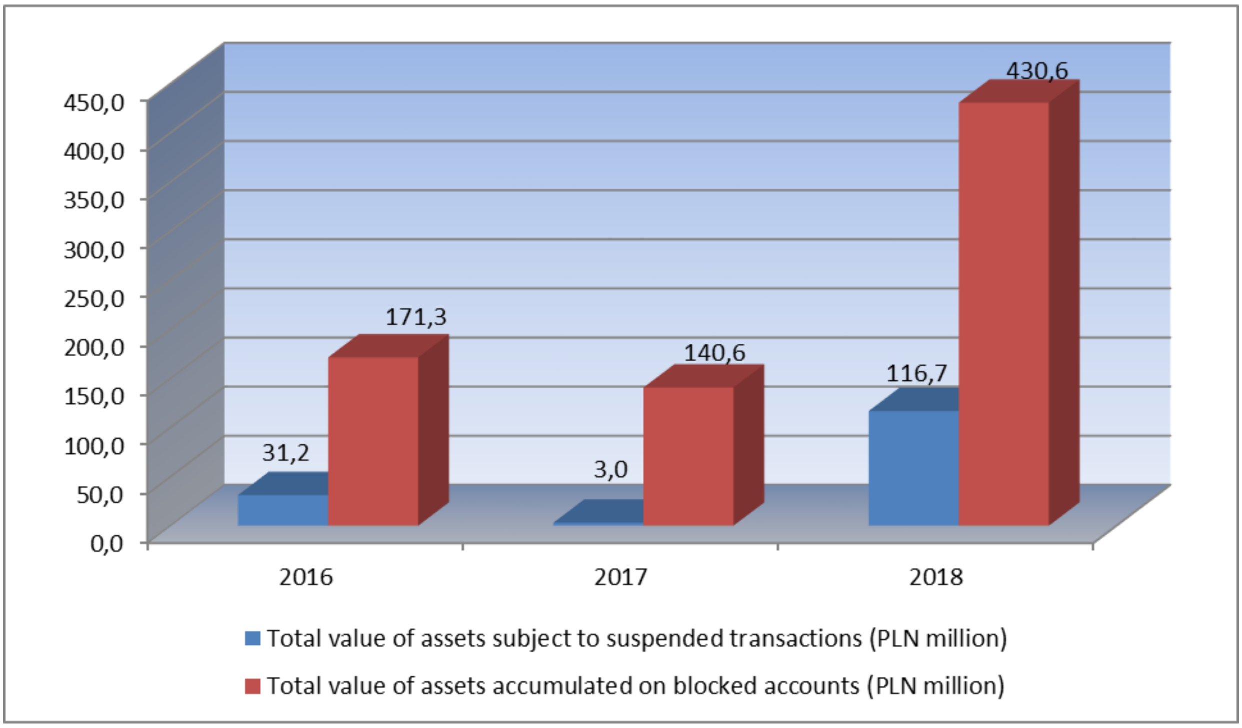
[421] Most of the cooperating units respond within the time frame set by the GIFI. There are occasionally cases where the GIFI does not receive a reply from a cooperating unit to the submitted request under Article 82(1) of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*.



859. The results of conducted analytical proceedings, such as the number of blocked account, suspensions of transactions, notifications to the public prosecutor's office or notifications to other public administration bodies, largely depend on individual analytical proceedings (inter alia: possibility and time-intensity of obtaining additional information confirming the suspicion of money laundering or financing of terrorism, time-intensity of the analysis of collected information, speed of transfer of the assets subject to analysis, number of entities, accounts and transactions to be verified and analysed). Therefore, some fluctuations of these data can be observed between individual years.

860. Information on the number of blocked accounts and suspensions of transactions would not be complementary without data on the total amount of assets stored on accounts blocked by the GIFI or the total value of suspended transactions.

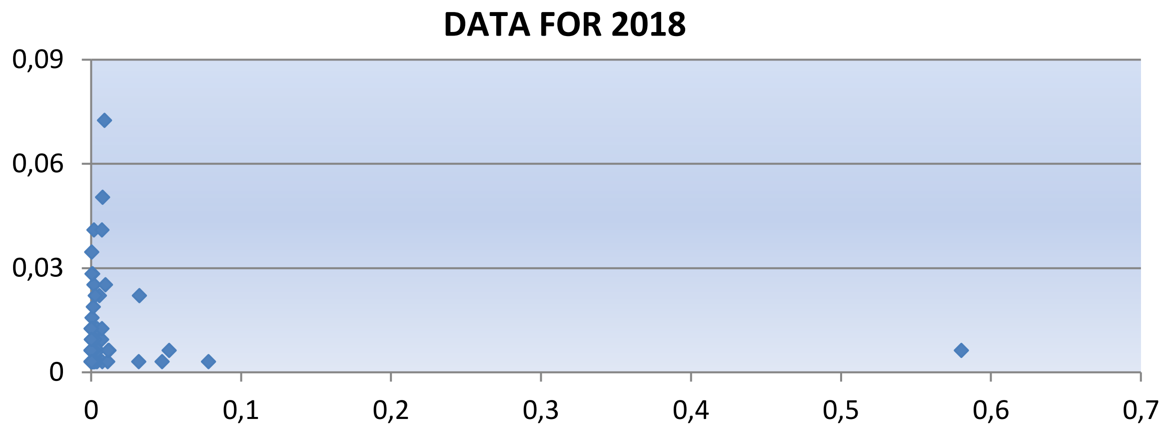
Figure no. 21 - Specification of assets accumulated on blocked accounts or subject to suspended transactions for 2016-2018



861. In 2018, a significant increase in the total assets accumulated on the accounts blocked by the GIFI was recorded as well as the total assets subject to transactions suspended by the GIFI. It is worth noting, however, that about 57.8% of the total assets accumulated on the accounts blocked by the GIFI in 2018 and about 59.0% of the total property values of the transactions suspended by the GIFI in 2018 concerned the blocking of accounts and suspension of transactions within one analytical procedure. The same case occurred in previous years, although it was not so visible at that time (more than a half of the total assets accumulated on blocked accounts was usually the result of measures undertaken in connection with several analytical proceedings). Also in the case of suspension of transactions, the execution of one or two analytical proceedings resulted in the suspension of transactions whose value exceeded half of the total assets subject to all transactions suspended in a given year.

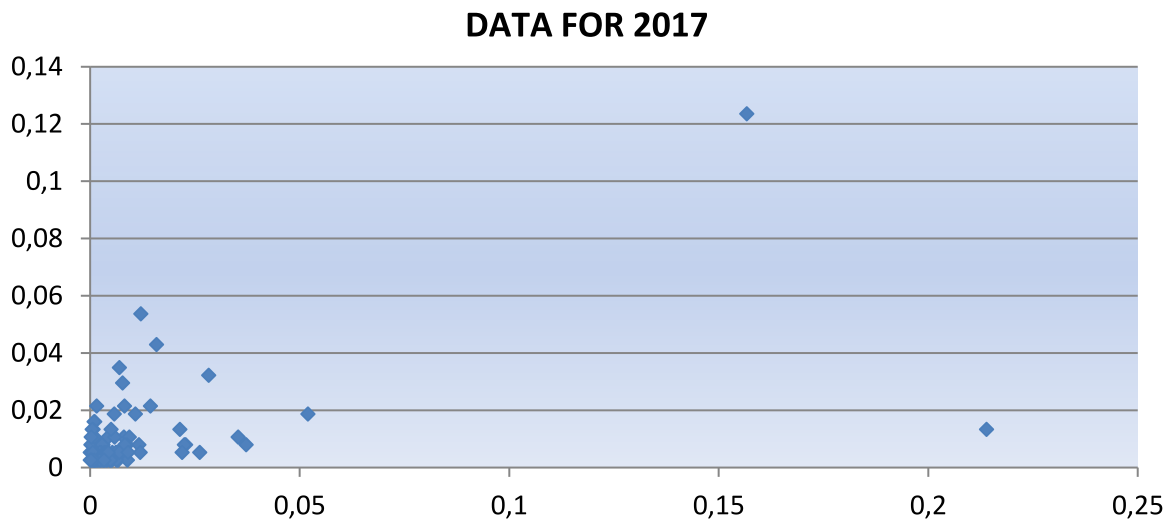
862. Taking into account jointly the blocking of accounts and suspension of transactions carried out in one year, more than a half of the total amount of assets related to those accounts and transactions concerned actions undertaken within the framework of approx. 0.9% to approx. 5.3% of all analytical proceedings in which the above mentioned legal instruments were applied in a given year.

Figure no. 22 - Distribution of assets accumulated on blocked accounts and subject to suspended transactions in relation to the number of analytical proceedings under which the GIFI applied these legal instruments in 2016-2018



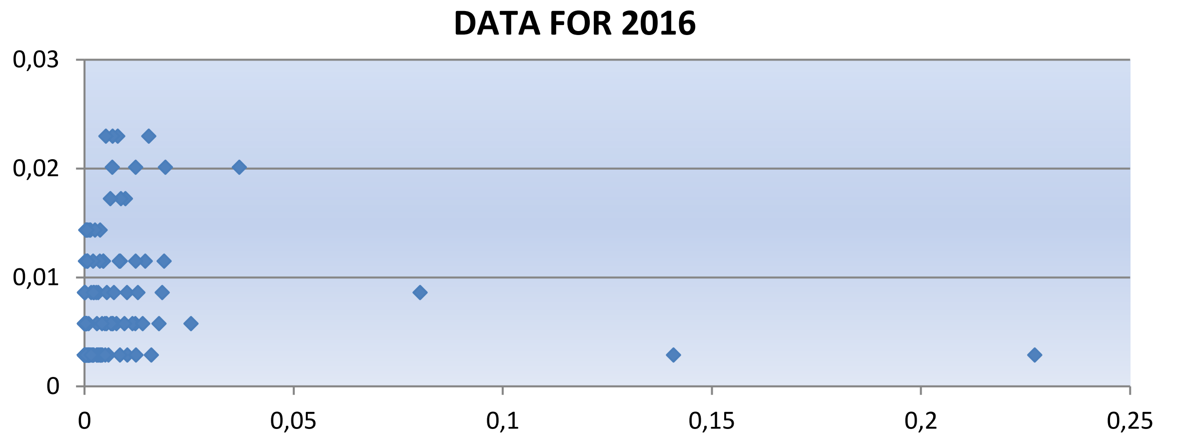
Axis X - share of assets accumulated on blocked accounts and assets subject to suspended transactions under single analytical proceedings in total assets accumulated on blocked accounts and assets subject to suspended transactions under all analytical proceedings

Axis Y - share of the number of blocked accounts and transactions suspended under single analytical proceedings in total number of blocked accounts and transactions suspended under all analytical proceedings



Axis X - share of assets accumulated on blocked accounts and assets subject to suspended transactions under single analytical proceedings in total assets accumulated on blocked accounts and assets subject to suspended transactions under all analytical proceedings

Axis Y - share of the number of blocked accounts and transactions suspended under single analytical proceedings in total number of blocked accounts and transactions suspended under all analytical proceedings



Axis X - share of assets accumulated on blocked accounts and assets subject to suspended transactions under single analytical proceedings in total assets accumulated on blocked accounts and assets subject to suspended transactions under all analytical proceedings
Axis Y - share of the number of blocked accounts and transactions suspended under single analytical proceedings in total number of blocked accounts and transactions suspended under all analytical proceedings

863. It should be remembered that as a result of the analyses carried out, only a part of analytical proceedings of the GIFI was properly justified to notify the prosecutor of the suspicion of money laundering. Moreover, only in the case of some of these analytical proceedings was it possible to block accounts or suspend transactions. Most of the analytical proceedings in which the GIFI applied these legal instruments were related to the blocking of one or more accounts or the suspension of one or more transactions. The total amount of assets accumulated on blocked accounts or subject to suspended transactions under a single transaction most often did not exceed 5% of the total assets accumulated on blocked accounts or subject to suspended transactions in a given year, under all analytical proceedings.

864. Within its area of competence, the GIFI shall communicate the information in its possession in response to requests sent by those cooperating units which are entitled to receive it[422].

[422] Currently, in accordance with Article 104 and 105 *of the Act of 1 March 2018 on counteracting money laundering and terrorist financing*, they include:
a) courts and prosecutors (for the purposes of pending criminal proceedings);
b) Chief Commander of the Police, Commander of the CBŚP, Chief Commander of the ŻW, Chief Commander of the SG, Chief Commander of the ABW, Head of the AW, Head of the AW, Head of the SKW, Head of the Military Intelligence Service, Head of the CBA, Internal Supervision Inspector, Chief of the Police Internal Affairs Office and Chief of the SG Internal Affairs Office or persons authorised by them (within the scope of statutory tasks of those bodies);
c) Chair of the Polish Financial Supervision Authority (KNF (PFSA)) – in the scope of oversight exercised by the KNF (PFSA) pursuant to *the Act of 21 July 2006 on the financial market oversight*);
d) President of the NIK – to the extent necessary to conduct audit proceedings defined in *the Act of 23 December 1994 on the Supreme Audit Office* (Journal of 2019, item 489);
e) the national administrator referred to in Article 3(22) of *Commission Regulation (EU) No 389/2013 of 2 May 2013 establishing a Union Registry pursuant to Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No 406/2009/EC of the European Parliament and of the Council and*

865. Most requests for information addressed to the GIFI as well as replies to them, are submitted without the intermediation of ICT systems.

866. In 2016, a decrease in the total number of applications from cooperating units was observed in relation to the data for the previous year. This was mainly associated with the decline in applications submitted by the bodies reporting to the Minister of Finance but also to the ABW, the Police, the SG and courts. In the years 2017-2018, the downward trend in the overall number of applications continued.

---

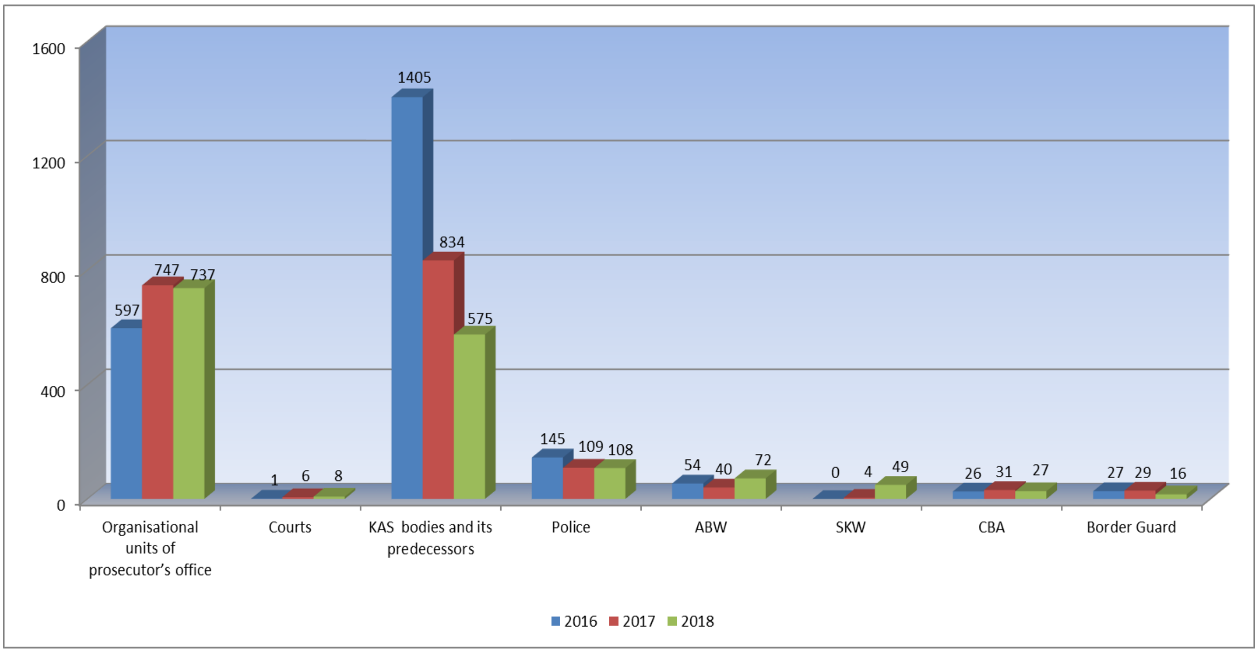
repealing Commission Regulations (EU) No 920/2010 and No 1193/2011 (OJ L 122, 03.05.2013, p. 1, as amended) - within the scope of its competence;

f) minister competent for foreign affairs – in the scope of its statutory competence in connection with the application of specific restrictive measures;

g) minister competent for public finance – in connection with the request referred to in Article 11(2) *of the Gambling Law of 19 November 2009*;

h) The head of the KAS, directors of the revenue administration regional offices or heads of customs and tax control offices (within the scope of their statutory tasks).

Figure no. 23 - Number of requests for information submitted to the GIFI from selected cooperating units under Article 32 or 33 of the Act of 16 November 2000 on counteracting money laundering and financing of terrorism or Article 104 or 105 of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2016-2018[423]



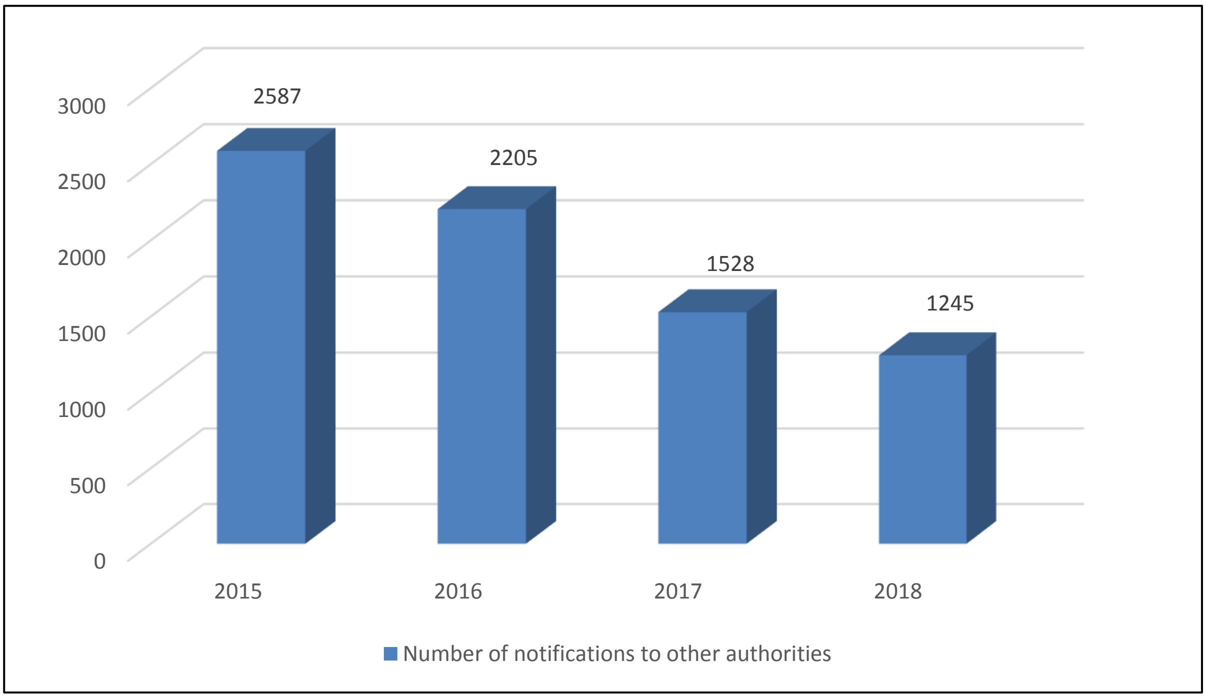
867. The GIFI strived to respond to the requests received as quickly as possible. In 2017, the estimated average time was about 10 days, and in 2018. - about 11 days. However, it should be noted that relatively often the replies were submitted very quickly, on the same day as the request was received. At the same time, in particular in cases where additional information, other than held by the GIFI on the date of receipt of the request, had to be collected for the reply, it could have taken even several months to provide a full reply to the request.

868. The GIFI also submits notifications to other public administration bodies, in particular law enforcement agencies. These were usually related to circumstances indicating that an offence other than money laundering was suspected as well as to the content of the information and requests provided by these entities.

869. The noticeable decrease in the number of notifications between 2015 and 2018 was mainly due to the decrease in the number of notifications submitted to the revenue control authorities (as well as tax and customs authorities) and since 2017 to the National Revenue Administration (KAS), which used to reached the highest number. The percentage share of these notifications in the total number of notifications was as follows: in 2015 they accounted for about 71.6%, in 2016 - 74.1%, in 2017 - 64.7% and in 2018, only 47.3%. The reduction of the number of notifications to the indicated recipients is related to the increasing effectiveness of the activities undertaken by the KAS in the field of combating tax crime as well as the development of tools enabling the KAS bodies to access and effectively analyse financial data.

[423]Based on information contained in: Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, p. 51 and 56.

Figure No. 24 - Data concerning notifications[424] submitted by the GIFI (for 2015-2018)[425]



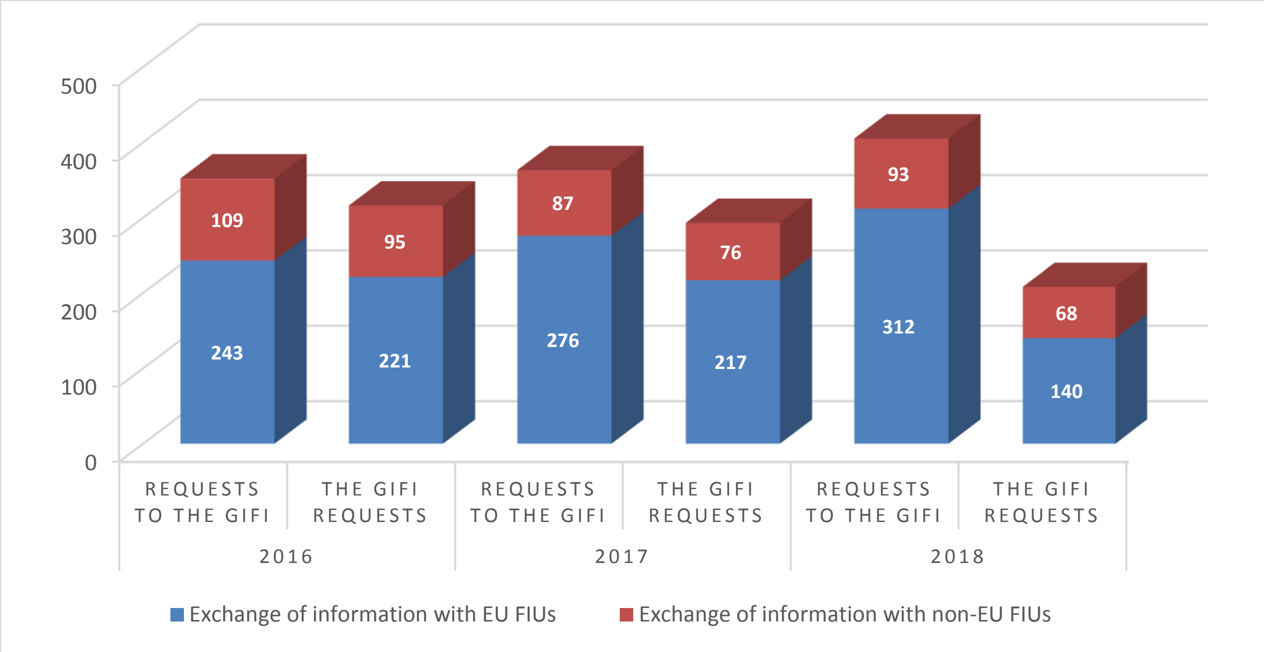
870. The GIFI exchanges information also with foreign financial intelligence units. Since 2015, the number of applications addressed to the GIFI from its foreign counterparts has remained at a relatively similar level (in 2016 its slight decline was noted compared to the previous year, i.e. by 5.1%, and in 2017 a relatively small increase - by 3.1%).

Figure no. 25 - Number of applications received and sent by the GIFI in the framework of information exchange with foreign FIUs in the years 2016-2018[426]

[424] Until 13 July 2018, submitted pursuant to Article 33(3) of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing* and after that date - pursuant to Article 106 of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*.

[425] Based on data presented in GIFI annual reports for 2015-2018, published on the website of the Ministry of Finance.

[426]Based on information contained in: Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2017, Warsaw 2018, pp. 56-59; Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2016, Warsaw 2017, pp. 53-56; Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, pp. 80-84.



871. Requests for information were most often transmitted by the EU FIUs. In 2018, more than 77% of the applications came from these units, with more than 49% of the applications from EU units forwarded by the FIUs from France, Germany, Latvia, Italy and the UK (in 2017, about 42% of such applications came from units from France, the UK, Germany and Latvia). Among the non-EU FIUs, units from Ukraine and Russia were most active in 2018 (as in the previous year)[427]. The GIFI strived to and continues to respond as quickly and comprehensively[428] as possible to the requests received. In 2017, the estimated average time was about 17 days, and in 2018, even shorter, i.e. about 12 days. In the case of a considerable part of the applications (more than ¼ in 2017 and about ¼ in 2018) replies were sent within 2 days.

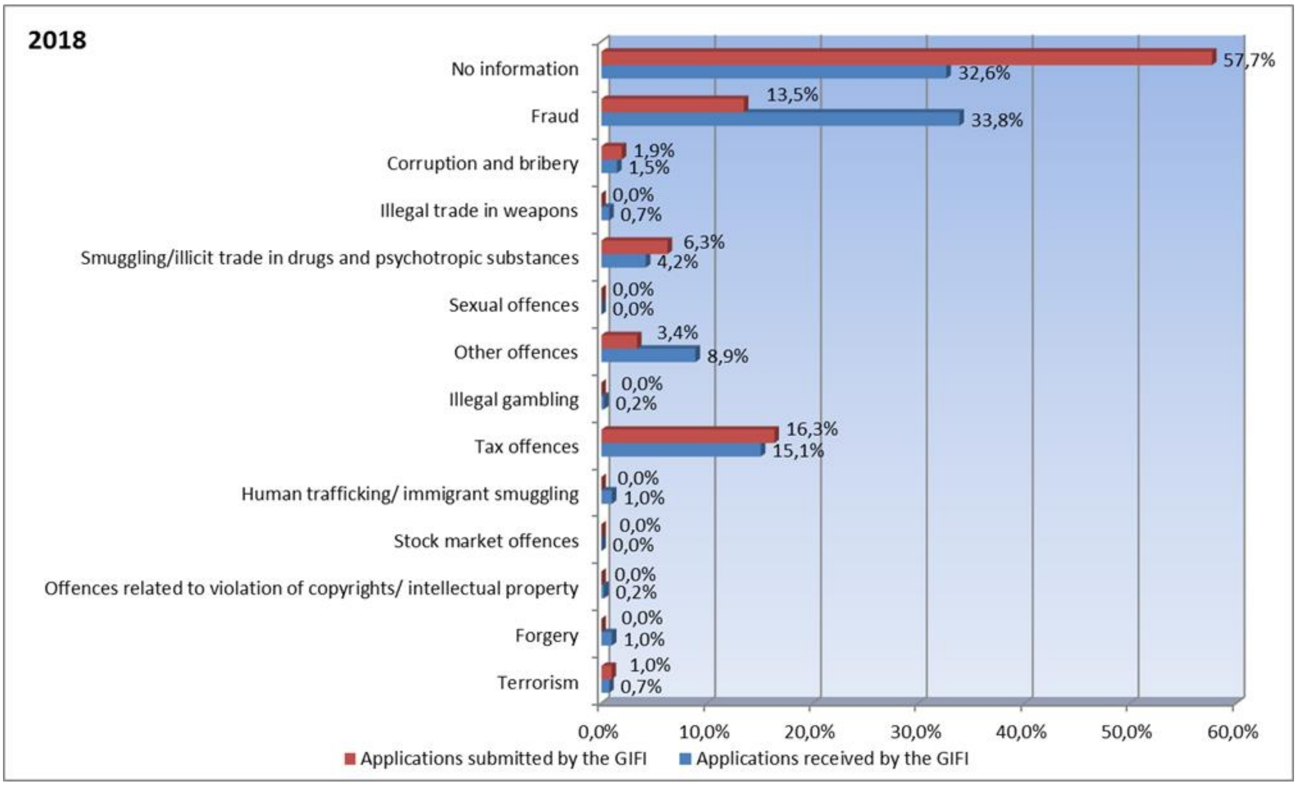
872. In addition to requests for information, the GIFI received so-called spontaneous information from foreign FIUs in the years 2016-2018. They were usually related to transactions of Polish entities or assets transferred to/from the territory of Poland. In 2018, there were 2,893 pieces of such information (632 in 2017 and 461 in 2016). The increase was mainly due to more information sent by the Dutch and Luxembourg FIUs.

873. In the years 2016-2018, the GIFI most frequently requested information from foreign FIUs from the EU[429] In 2018, it sent over 67% of all applications to them. Nearly 44% of applications to the EU FIUs were addressed to entities from 4 countries: Latvia, the United Kingdom,

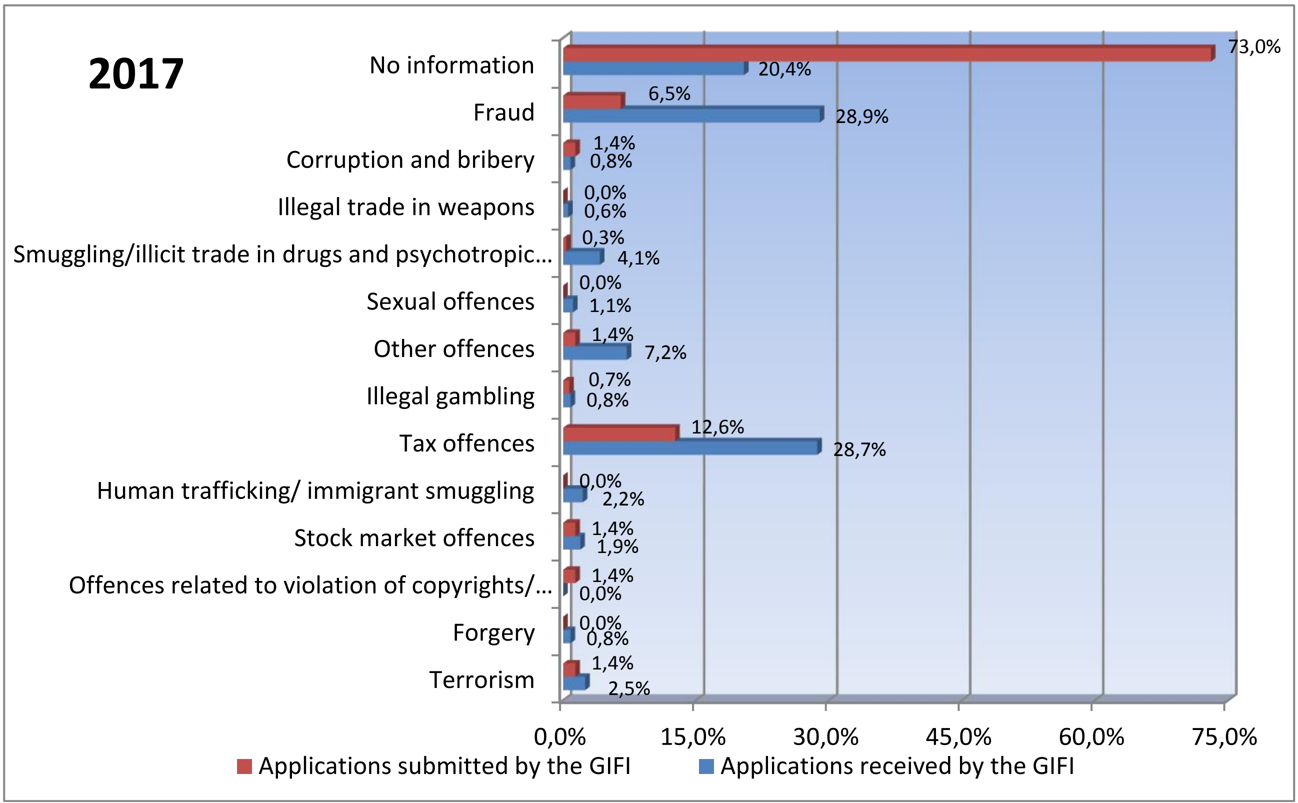
[427] Report of the General Inspector of Financial Information on the implementation of the *Act of 16 November 2000 on counteracting money laundering and terrorist financing* and the *Act of 1 March 2018 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, p. 81.
[428] The current provisions of *the Act of 1 March 2018 on counteracting money laundering and terrorist financing* indicate that the provision of Article 99(7) of the aforementioned Act does not apply to the information made available to foreign FIUs, with the exception of the provisions on the protection of classified information (Article 111(5) of the aforementioned Act). Potential situations where the GIFI may refuse to provide information have been defined in Article 114(1) of the aforementioned Act.
[429] The timing of the response was largely dependent on the requested FIU, its powers to obtain information. It is estimated that in 2018 the average response time was about 19.3 days.

Germany and the Czech Republic. In the case of non-EU FIUs, the GIFI forwarded the highest number of applications to the Ukrainian unit in 2017, i.e. over 38% of all applications to these FIUs.[430]

Figure no. 26 - Estimated distribution of applications from and to foreign FIUs according to potential predicate offences in 2017-2018[431]



[430] At the same time, the FIU from Ukraine was the recipient of the highest number of applications among all FIUs (both EU and non-EU).
[431] According to its own information on the exchange of information with foreign FIUs (one request could relate to money laundering from several types of crime).



874. An analysis of the content of requests received by the GIFI from foreign FIUs in the years 2017-2018 shows that they most often concerned suspected money laundering from predicate offences such as fiscal offences and fraud (although in a large part of the cases they did not contain information about a potential predicate offence). Similar situation occurred in the case of requests sent by the GIFI, although with a significant number of them it was not possible to indicate the potential predicate offence.

875. It is worth noting that not all foreign FIUs have similar powers in the scope of access to information at the national level. Some of them do not have access to all the financial information processed in their countries, especially this that goes beyond the information reported in the STR, SAR or in above-threshold transactions collected by these FIUs[432]. Thus, it is not always possible for the GIFI to obtain all the information needed to assess the suspicions of money laundering or financing of terrorism from these entities.

876. The GIFI also sends spontaneous information to foreign FIUs[433]. In 2018, it provided 16 pieces of such information (addressed to the FIUs from the following countries: Estonia, the

[432] Some FIUs may not request the history of an account from their obligated institutions if no SAR/STR has previously been sent by that institution concerning an entity associated with the account or a SAR/STR from any other obligated institution concerning the entity covered by the request.

[433] Pursuant to Article 53(1) of Directive 2015/849, where a FIU receives a STR/SAR relating to another EU Member State, it is required to transfer it to the FIU of that Member State without delay. The aforementioned provision was implemented by means of Article 112(3) of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing.* On its basis, the GIFI sends cross-border reports in a structured form through the FIU.NET network, i.e. the information exchange system between EU financial intelligence units. The GIFI also receives reports from other Member States and links them to information in its possession. Currently, within

Netherlands, Ireland, Lithuania, Latvia, Moldova, Portugal, Slovakia, Switzerland, Ukraine, the United Kingdom).[434]

877. In addition to its typical FIU responsibilities, the GIFI also performs tasks which do not always fall within the competence of these entities. Among others, it exercises the control of compliance of the obligated institutions with the obligations in the scope of counteracting money laundering and financing of terrorism. In the years 2016-2017, the GIFI carried out the total of 40 such inspections, and in 2018 - 8 inspections.

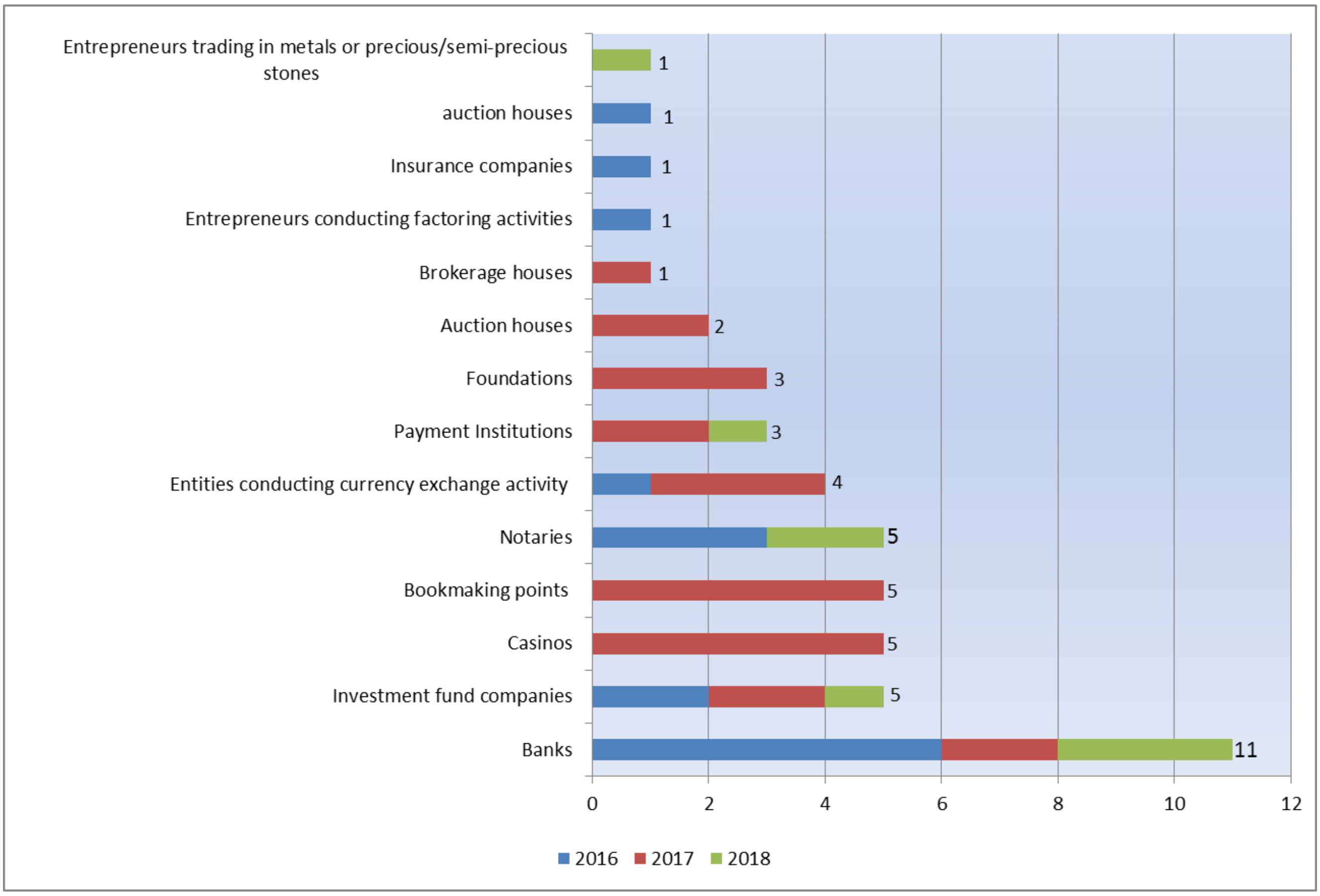
878. As Figure no. 27 shows, every year there has been an attempt to carry out inspections in the obligated institutions belonging to different categories, with the choice of these categories rarely being repeated. The total number of inspections carried out depends on the staffing capacity of the unit of the Financial Information Department of the Ministry of Finance, which performs, among others, such tasks. In addition, less inspections were carried out in 2018 than in previous years due to the entry into force of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* at the beginning of the second half of 2018. Therefore, in the second half of 2018, the GIFI did not carry out inspections in order to give time to the obligated institutions to implement the regulations properly, by adjusting internal regulations and procedures and introducing adjustment measures.

---

the FIU.NET Advisory Group a working group operates to improve the effectiveness of the cross-border reporting system.

[434] Report of the General Inspector of Financial Information on the implementation of the *Act of 16 November 2000 on counteracting money laundering and terrorist financing* and the *Act of 1 March 2018 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, p. 83.

Figure no. 27 - Number of GIFI inspections in obligated institutions in the years 2016-2018[435]



879. The GIFI also conducts administrative investigations concerning imposing of administrative penalties on obligated institutions that are committed to comply with their obligations under anti-money laundering and counter-terrorist financing legislation. Until 13 July 2018, the GIFI was the only authority authorised to impose fines for such infringements[436].

880. In 2017, the GIFI conducted 99 administrative proceedings (i.e. approx. 22.2% more than in 2016), with approx. 10.1% based on the results of its own inspections and approx. 89.9% based on the results of inspections carried out by other authorised bodies.[437] Also in 2016, the majority of administrative proceedings were initiated on the basis of the findings of controls of other authorised bodies (approx. 84.0%).[438]

---

[435]Based on information contained in: Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2017, Warsaw 2018, p. 31; Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 *on counteracting money laundering and terrorist financing* in 2016, Warsaw 2017, p. 29; Report of the General Inspector of Financial Information on the implementation of the *Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, p. 46.

[436] *The Act of 16 November 2000 on counteracting money laundering and terrorist financing* provided for only one type of administrative penalty, i.e. a fine.

[437] Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2017,* Warsaw 2018, p. 34.

[438] Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2016,* Warsaw 2017, p. 31.

881. In 2018, pursuant to the provisions of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism,* the GIFI conducted 49 administrative proceedings concerning imposing fines on obligated institutions for the failure to comply with the provisions of the Act (including about 16.3% based on the findings of own inspections).

882. Moreover, in 2018 the GIFI submitted 3 notifications to the Prosecutor's Office on committing offences which exhaust the features of acts specified in Article 35 of *the Act of 16 November 2000 on counteracting money laundering and financing of terrorism* (in 2017 - 18 such notifications were sent).[439]

883. The GIFI operates under the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the Financial Security Committee which exercises an advisory and opinion-forming function in the field of anti-money laundering and counter-terrorist financing, consisting of representatives of the main public administration bodies operating in the national anti-money laundering and counter-terrorist financing.[440] In its framework, *the Working Group to identify and analyse information and documents in order to fulfil the obligation referred to in Article 26 of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* was established whose work has contributed significantly to the development of this national risk assessment of money laundering and financing of terrorism. Moreover, in May 2019 the Committee adopted the *Resolution concerning establishing the Working Group for cooperation of representatives of the public, private and public-private sectors.* In accordance with the content of this resolution, the working group has been established whose tasks comprise:

- advising on the implementation of the tasks of the Committee referred to in Article 19(2) of the aforementioned Act;
- exchange of knowledge and experience arising from the implementation of statutory tasks in the field of identifying, preventing and combating money laundering and financing of terrorism as well as other related prohibited acts.

7.3.3. Activities of law enforcement agencies

884. The law enforcement agencies usually include the prosecutor's offices, the Police, the Military Police, the CBA, the ABW, the Border Guard and the Customs and Tax Control Service, operating within the KAS. For the purposes of this analysis, all those bodies, institutions and services dealing with investigation/combating of offences which are listed in Article 105(1) and (4) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, have been included in the aforementioned bodies.

885. In response to one of the questions included in the questionnaires distributed by the GIFI in the second half of 2017, the majority of respondents, representing law enforcement agencies[441] who answered this question indicated that financial and equipment resources needed

[439] Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing* in 2018, Warsaw 2019, p. 47*;* Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing in 2017,* Warsaw 2018, p. 33.

[440] The composition of the Committee is presented in subchapter 4.3.1.

[441] 7 completed questionnaires were received, submitted by representatives of: the National Prosecutor's Office, the Police, the CBŚP, the ABW, the SG and the CBA.

to carry out tasks related to counteracting and combating money laundering were sufficient (42.9% of all respondents; 28.6% of all respondents indicated that they were not). On the other hand, in the case of human resources, the majority of respondents defined them as insufficient (about 42.9% of all respondents) and 28.6% of all respondents indicated that they were not satisfactory. The lack of trained experts, officers with relevant professional experience and staff turnover were indicated as the justification.

886. Answers to the question related to sufficient resources for the implementation of tasks in the scope of counteracting money laundering and financing of terrorism were slightly different. The majority of respondents who answered this question indicated that the equipment and human resources needed to carry out tasks in the above mentioned area were adequate (42.9% of all respondents for each question, respectively; 28.6% of all respondents indicated that the equipment resources were not sufficient and 14.3% described the human resources as insufficient). On the other hand, in the case of financial resources, the majority of respondents defined them as unsatisfactory (about 42.9% of all respondents) while 14.3% of all respondents indicated that they were satisfactory.

887. Powers of law enforcement agencies arising from anti-money laundering and counter-legislation were extended as a result of legislative changes in 2018. Among others, the limitation in obtaining information from the GIFI on a written and justified request concerning above-threshold transactions by law enforcement authorities (except for the prosecutor's office, to which it did not apply), i.e. having the consent of the General Prosecutor to request for this type of data[442], was eliminated.

888. Moreover, *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* directly indicates the authorities and units which may obtain information from the GIFI within the scope of their statutory tasks, listing - next to the Head of the ABW, the AW, the SKW, the SWW and the CBA - among others those which are supervised by the minister competent for internal affairs, i.e.: the Chief Commander of the Police, the Commander of the Central Police Investigation Bureau, the Commander of the Office for Internal Affairs of the Police, the Commander of the Office for Internal Affairs of the Border Guard and the Internal Supervision Inspector. The Chief Commander of the Military Police was also added to this catalogue[443] A separate paragraph also provides for the possibility of obtaining information from the GIFI by the Head of the KAS, directors of revenue administration regional offices and heads of customs and tax control offices in connection with the performance of their statutory tasks.[444]

889. At the same time, the GIFI was committed to inform prosecutors about the possession of information (not only this provided to the obligated institutions and cooperating units with regard to the suspicion of money laundering or financing of terrorism or occurrence of circumstances which may indicate a suspicion of money laundering or financing of terrorism but also information about above-threshold transactions) related to the information provided by them about issuing an order to block an account or suspend a transaction, about commencing

[442] Article 33(4) of the *Act of 16 November 2000 on counteracting money laundering and terrorist financing.*
[443] Article 105(1) of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*.
[444] Article 105(4) of the aforementioned Act.

the proceedings, presenting a charge and filing a bill of indictment, in cases under Articles 299 and 165a of the kk[445].

890. The GIFI is also obliged to send information to law enforcement agencies about the suspected fiscal offences or offences other than money laundering or financing of terrorism.[446]

891. Individual law enforcement agencies have different responsibilities and powers.

892. In accordance with Article of *the Act of 28 January 2016 Law on the Public Prosecutor's office* - (Journal of Laws of 2019, item 740), the tasks of the prosecutor 's office[447] include:

1) conducting or supervising preparatory proceedings in criminal matters and exercising the function of a public prosecutor before the courts;
2) bringing actions in civil cases and submitting applications and participating in legal proceedings in civil cases, in the scope of labour and social security law, where the protection of the rule of law, social interest, property or citizens' rights so requires;
3) to take measures provided for by law, aimed at the correct and uniform application of the law in judicial and administrative proceedings, in cases of offences and in other proceedings provided for by Act;
4) exercising supervision over the execution of decisions on pre-trial detention and other decisions involving deprivation of liberty;
5) conducting research on the issues of crime and its combating and prevention, as well as cooperation with the entities referred to in Article 7(1)(1), (2) and (4)-(8) *of the Act of 20 July 2018 - Law on higher education and science* (Journal of Laws, item 1668, as amended), in the scope of conducting research on the issue of crime, its combating and prevention and control;
6) collecting, processing and analysing in IT systems the data, including personal data, originating from the proceedings conducted or supervised under the Act and from participation in court and administrative proceedings, in cases of an offence or other proceedings provided for by the Act, transferring the data and results of analyses to the competent authorities, including authorities of another country, if provided for by the Act or an international agreement ratified by the Republic of Poland;
7) challenging to the court and participating in court proceedings concerning the legality of administrative decisions that are unlawful;
8) coordination of activities in the field of prosecution of offences or tax offences carried out by other state authorities;

---

[445] Article 81(4) of the aforementioned Act.

[446] Article 106(1) of the *Act of 12 March 2018 on counteracting money laundering and terrorist financing*. Pursuant to Article 106(2) of the aforementioned Act, the GIFI is obliged to inform the KNF (PFSA) about cases of a justified suspicion of a breach of regulations related to the functioning of the financial market,

[447] The public prosecutor's office is composed of the General Prosecutor (the chief public prosecutor's authority), the National Prosecutor, other deputies of the General Prosecutor and public prosecutors of the common organisational units of the public prosecutor's office (i.e. the public prosecutors of the National Prosecutor's Office, regional prosecutor's offices and district prosecutor's offices) and the prosecutors of the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation, hereinafter referred to as the "Institute of National Remembrance" (Article 1 of *the Act of 28 January 2016 - Law on the Public Prosecutor's office*).

9) cooperation with state authorities, state organisational units and social organisations in preventing crime and other infringements of law;

10) cooperation with the Head of the National Centre of Criminal Information (KCIK) to the extent necessary to carry out its statutory tasks;

11) cooperation and participation in activities undertaken by international or supranational organisations and international teams, acting under international agreements, including agreements that constitute international organisations, ratified by the Republic of Poland;

12) preparing opinions on draft internal acts of law;

13) cooperation with organisations associating prosecutors or prosecutors' employees, including co-financing of joint research or training projects;

14) taking other actions specified in the Acts.

893. The General Prosecutor, as the chief public prosecutor's office, manages the activities of the public prosecution service in person or through the National Prosecutor and other Deputy Prosecutors-General, issuing orders, guidelines and instructions[448] Among others, in 2016 it issued guidelines on the principles of conducting preparatory proceedings for financial crimes committed to the detriment of many affacted parties using financial instruments and banking activities[449]

894. The structure of the Prosecutor's Office foresees four levels of hierarchically subordinate units, namely, Local Prosecutor's Offices, District Prosecutor's Offices, Regional Prosecutor's Offices and National Prosecutor's Office. It is worth mentioning that in 11 regional prosecutor's offices there are departments for economic crime and in the largest units there are 6 additional departments for financial and tax crime. In addition, 32 out of 45 District Prosecutor's Offices have established business departments and in the remaining 13 units financial and tax crime departments operated. On the other hand, the National Prosecutor's Office includes, inter alia, the Department for Economic Crime, which supervises and coordinates the prosecution of economic and financial and tax crime (in particular, related to VAT fraud and cybercrime), as well as the Department for Organised Crime and Corruption, which supervises the work of 11 Local Divisions where the most serious investigations into organised crime, corruption and terrorist offences are conducted.

895. The Prosecutor's Office also conducts preparatory proceedings related to suspected money laundering or financing of terrorism offences. In 2018, 608 pre-trial proceedings were initiated in money laundering cases[450] In that period, preparatory proceedings were pending in cases concerning money laundering, in which 3310 persons were charged under Article 299§ 1 of the *Penal Code*, and 11 persons were charged under Article 299§ 2 of the *Penal Code*. Moreover, 209 cases concerning money laundering were closed with a bill of indictment, 14 with a motion for a conviction and 135 with discontinuance. Initiation of preparatory proceedings was refused in 40 cases

[448] Article 1§1 of *Act of 28 January 2016* - Law on the Public Prosecutor's office.
[449] https://pk.gov.pl/dzialalnosc/wytyczne-i-zarzadzenia/wytyczne-i-zarzadzenia/, date of reading 6 June 2019
[450] Report of the General Inspector of Financial Information on the implementation of the Act of 16 November 2000 on counteracting money laundering and terrorist financing and the Act of 1 March 2018 on counteracting money laundering and terrorist financing in 2018, Warsaw 2019, pp. 58-59.

896. The Police are composed of a number of units, some of which are specialised in implementing activities in their specific areas of interest. It comprises: The Police Headquarters (KGP), the Central Bureau of Investigation of the Police (CBŚP), the Office of Internal Affairs of the Police, 16 provincial Police Headquarters, the Capital City Police Headquarters, the Central Counter-Terrorist Subdivision of the Police - "BOA", the Central Forensic Laboratory of the Police and 5 police schools.

897. Within the KGP, among others, the KGP Criminal Office operates which includes, among others, the Property Recovery Department. The tasks of the above mentioned department include:

- carrying out the tasks of the National Asset Recovery Office;
- exercising supervision over the performance by entities and organisational units of the Police of tasks in the scope of detection and identification of property resulting from crime or other property related to crime;
- cooperation with national entities with powers to disclose, identify, protect and recover assets;
- conducting international cooperation concerning the issues of disclosure, identification, freezing and recovery of assets derived from or linked with crime, in particular the activities of the Camden Assets Recovery Inter-Agency Network (CARIN) and other similar international initiatives;
- developing proposals for amendments to the legislation governing the disclosure, identification, freezing and recovery of assets derived from or linked with a criminal offence;
- organising and participating in the professional development of police officers within the scope of departmental competence.

898. Another department operating in the KGP Criminal Office is the Department for Combating Economic Crime. Its tasks include:

- identifying, monitoring and analysing areas at risk of economic crime across the country;
- developing and implementing guidelines and ways to effectively identify, prevent and disclose economic crime;
- inspiring, coordinating and supervising operational, exploratory and investigative activities within the scope of the department's competence;
- providing support and direct assistance to police organisational units combating economic crime in carrying out operational, exploratory and investigation activities;
- conducting national cooperation with law enforcement agencies and the judiciary, public administration bodies, social organisations and representatives of other entities as regards counteracting and combating economic crime;
- conducting international cooperation with authorised entities in the scope of implementation of tasks aimed at combating economic crime;

- acquiring and transmitting information on committed economic crime to provincial (Capital) Police Headquarters;
- participating in preparing the opinions on draft legislation concerning the economic crime;
- issuing opinions on requests for access to classified materials within the scope of operational work used by police organisational units combating economic crime;
- participation in meetings of national and international working groups, task forces and contact points;
- participation in conferences, training activities, seminars and training workshops to promote knowledge on preventing and combating economic crime;
- organising and participating in the professional development of police officers within the scope of the department competence;
- conducting operational and exploratory activities within the scope of the department competence.

899. In the case of the CBŚP, its tasks include, in particular, planning, coordinating and undertaking measures aimed at identifying and preventing national and international organised crime, in particular of criminal, drug and economic nature. In terms of counteracting economic crime, the CBŚP undertakes activities comprising, among others:

- identifying, revealing and combating organised economic crime, with particular focus on VAT fraud in the area of trade in various types of goods, including, with international range;
- identifying, revealing and combating organised crime, including international crime, related to smuggling, illicit trafficking of tobacco and tobacco products and the discovery and dismantling of illegal tobacco production sites;
- combating organised crime and serious crime to the detriment of financial market institutions;
- combating organised fraud in economic transactions, including to the detriment of the EU's financial interests;
- identifying, counteracting and combating money laundering from organised crime and undertaking legal actions to recover property from the perpetrators.

900. Pursuant to Article 15 of *the Act of 6 April 1990 on the Police* (Journal of Laws of 2019 item 161 as amended) in the framework of conducted cases concerning money laundering, the Police may turn to institutions providing payment services. Moreover - pursuant to Article 20(3) of the aforementioned Act, if it is necessary for effective prevention of offences or their detection, determination of their perpetrators, obtaining and recording evidence as well as the detection and identification of objects and other property benefits derived from these crimes or their equivalent - on the basis of a court decision issued on request of, among others, the Commander of the CBŚP, the Police may also use information constituting a tax secret, professional secrecy specified in acts on the functioning of the financial market, as well as information constituting individual data specified in the Act on the Social Insurance System. Moreover, in connection with Article 20(5a) of the aforementioned Act, on the basis of an

application of a competent authority or a person authorised by it, the Police may obtain other types of information and data:

- concerning the documentation related to assigning the NIP (Tax Identification Number) and updating the data contained in the identification notifications, (Act on the principles of registration and identification of taxpayers and payers);
- contained in files which do not include information referred to in Article 182 of *the Act of 29 August 1997 - Tax Ordinance* (Journal of Laws of 2018, item 800 as amended)'
- concerning the conclusion of an agreement with a natural or legal person or an organisational unit without legal personality to perform the activities referred to in Article 5 of *the Act of 29 August 1997 - Banking Law* or activities referred to in Article 3 of *the Act of 5 November 2009 on cooperative savings and credit unions*, enabling verification of the conclusion of such agreements and their duration,
- concerning the coverage of a natural person by social insurance and the amount of indexed pension insurance contributions premiums for a natural person as well as the data of the contribution payer referred to in Article 40, Article 45 and Article 50 of *the Act of 13 October 1998 on the social insurance system* (Journal of Laws of 2019, item 300 as amended);
- required to determine whether a natural or legal person as well as an entity without legal personality, has carried out transactions concerning the exchange commodities referred to in *the Act of 26 October 2000 on Commodity Exchanges*;
- necessary to establish whether a natural or legal person as well as an entity without legal personality, is a participant in an investment fund referred to in *the Act of 27 May 2004 on investment funds and alternative investment fund management*;
- concerning the determination whether a natural or legal person as well as an entity without legal personality, is a party to an agreement concerning trading in financial instruments;
- concerning the determination whether a natural or legal person as well as an entity without legal personality, is the policyholder, insured or beneficiary under an insurance contract within the meaning of the provisions of *the Act of 11 September 2015 on Insurance and Reinsurance Activity.*

901. Within the framework of access to the databases, the Police, including the CBŚP, use data sets maintained by various public administration bodies as well as the system of international information exchange with Europol - SWIZE.

902. The pragmatism of cases conducted by the Police on a crime under Article 299 of the Penal Code usually results in two directions of conducting operational and procedural activities:

- on the basis of the collected materials of an operational procedure/ case on the predicate offence (VAT fraud, credit extortion, illegal trade in narcotic drugs or psychotropic drugs), elements consisting in committing the primary predicate offence are disclosed;

- the authority conducting the investigation/operational case acquires information concerning suspicious transactions e.g. carried out on bank accounts and an important task in the course of conducted activities is to prove the predicate offence.

903. In connection with such a model, both officers of the division for combating organised drug crime, criminal or economic crime can carry out operational and procedural activities aimed at proving this crime.

904. In the years 2007-2014, a structure of coordinators responsible for the disclosure and securing the property was created within the CBŚP, outside the regular personnel (as of 26 November 2018 there were 62 coordinators). This is determined by the staffing situation, with regard to the number of investigations and operational cases conducted in the Bureau. The coordinator's task is to carry out checks in the EKW[451] databases, provide substantive assistance to officers in difficult and complex legal cases, provide opinions on documents related to cooperation with the GIFI as well as organise training on the subject of disclosing and securing property.

905. The Police, including the CBŚP, shall cooperate with other countries' police forces, as well as with national and international public administration services and offices, in areas and to the extent necessary to effectively combat and prevent organised crime.

906. International operational cooperation comprises primarily the exchange of information through:

- The Schengen Information System (SIS) and the National SIRENE Bureau (for the Schengen States);
- Europol;
- INTERPOL;
- cooperation within the network of Polish Police liaison officers operating in other countries as well as with foreign liaison officers accredited in Poland;
- direct access to police databases (missing and wanted persons, palmprint cards, DNA profiles, stolen vehicles and documents etc.).

907. In the Polish Police, the KGP Police International Cooperation Office is the contact point and the place where all international police information exchange channels converge. It coordinates and oversees all international non-operational, operational and training cooperation activities.

908. As regards the activities of the Border Guard as a law enforcement authority, there are three main groups of offences which it is entitled to prosecute:

- illegal migration;
- forgery of documents authorising to cross the state border of the Republic of Poland and their use as well as the theft or misappropriation and use of documents confirming the identity of another person and also concealing documents;

[451] Abbreviation for Electronic Land and Mortgage Register

- illegal movement of narcotic drugs, excise goods, weapons and ammunition, cultural goods etc. across the Polish border.

909. Moreover, in connection with the provisions of *the Act of 12 December 2013 on foreigners*, which introduced a number of new regulations in the area of proceedings with foreigners, the Border Guard gained a direct mandate to recognise, prevent and detect crime of human trafficking and slavery and to prosecute their perpetrators, which corresponds to the tasks that have been performed by the Border Guard for years.

910. In cases which fall within the material competence of the Border Guard, its officers may use the so-called "offensive working methods" in the form of operational control, controlled purchase or secretly supervised shipment.

911. Money laundering procedure is a phenomenon commonly occurring in the activity of organised criminal groups committing prohibited acts, which lie, inter alia, within the scope of statutory tasks of the Border Guard (area of illegal migration, smuggling of excise goods, smuggling of narcotic drugs and psychotropic substances). The Border Guard has no direct material competence to carry out operational, exploratory and investigation activities in the scope of combating the crime referred to in Article 299 of the kk, however, this crime may be covered by operational and exploratory activities, and as a consequence, the initiation of preparatory proceedings and the presentation of charges under this Article, in addition to the predicate offence, which lies within the competence of the Border Guard.

912. With a view to effective combating and preventing money laundering, on 11 September 2009 the Deputy Commander of the Border Guard approved the concept on "Conducting activities in the field of determining assets coming from illegal or undisclosed sources by Border Guard officers".

913. There are no separate organisational units in the Border Guard which would deal only with financial (economic) crime. In the framework of each pending pre-trial and operational case, the aim is to identify the income of the perpetrators of the offences and to deprive the profits made by the criminal groups.

914. On a strictly working level, in the course of specific cases, the Border Guard shall carry out working cooperation with liaison officers of other countries. In addition, at the working (operational) level, the Border Guard cooperates with Europol and INTERPOL.

915. The CBA is a special service established to combat corruption in public and economic life, in particular in state and local government institutions as well as to combat activities detrimental to the state economic interests. Its tasks include, in particular, the identification, prevention and detection of offences associated with corruption[452] and the prosecution of their perpetrators, and moreover:

- disclosure and prevention of cases of non-compliance with the provisions on restrictions on business activity by persons performing public functions;

[452]i.e. listed in Article 2(1)(1) of the *Act of 9 June 2006 on the Central Anti-Corruption Bureau* (Journal of Laws 2018, item 2104, as amended).

- documenting the grounds and initiating the implementation of regulations on the return of benefits wrongly obtained at the expense of the State Treasury or other state legal persons;
- disclosing cases of non-observance of the procedures for making and implementing decisions, as defined by law, concerning: privatisation and commercialisation, financial support, awarding public contracts, disposal of property of public finance sector entities, entities receiving public funds, entrepreneurs with the share of the State Treasury or local government entities, granting concessions, permits, subjective and objective exemptions, licences, preferences, quotas, ceilings, bank sureties and guarantees;
- control of the correctness and truthfulness of asset declarations or declarations of business activity submitted persons performing public functions;
- conducting analytical activities concerning phenomena occurring within the area of competence of the CBA and presenting information in this respect to the Prime Minister, the President of the Republic of Poland, the Sejm and the Senate**.**

916. Operational and exploratory activities are carried out by CBA officers in order to prevent crime, identify and detect offences as well as to obtain and process information essential for combating corruption in state institutions and local government, and activities detrimental to the economic interests of the state. If there is a justified suspicion of committing an offence, officers of the CBA perform investigation and prosecution actions set forth in the provisions of *the Code of Criminal Procedure*, including activities ordered by the court and the prosecutor.

917. Moreover, the CBA also carries out analytical and information activities in order to identify threats that are detrimental to the economic interest of the state and to inform the authorities of the state, if possible in advance, as well as to formulate possible proposals for remedial action. Furthermore, they support operational, exploratory, investigation and control activities.

918. Every year the CBA prepares - in cooperation with other services, the General Prosecutor's Office and the Ministry of Justice - and issues a report called *the Corruption Map.* It presents the status of corruption crime in Poland.

919. In accordance with Article 3 of *the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency*, the Head of the ABW is the central body of governmental administration, acting with the assistance of the ABW. The tasks of the ABW include, in particular:

1) Identifying, preventing and combating threats to the internal security of the state and its constitutional order, in particular its sovereignty and international standing, independence and integrity of its territory as well as the defence of the state.
2) Recognition, prevention and detection of, inter alia, the following crime:

- spying;
- terrorism;
- unlawful disclosure or use of classified information;
- corruption of persons performing public functions;

- offences in the area of production and trade in goods, technologies and services of strategic importance for state security;
- illicit manufacture, possession and trafficking of weapons, ammunition and explosives, weapons of mass destruction and narcotic drugs and psychotropic substances, in international trade.

3) Identification, prevention and detection of threats to security, ICT systems of public administration bodies relevant for the continuity of functioning of the state.
4) Performing the function of a national security authority for the protection of classified information in international relations.
5) Obtaining, analysing, processing and communicating to the competent authorities information that may be relevant for the protection of the internal security of the state and its constitutional order.

920. In cases falling within the material competence of the ABW it is possible to carry out operational, exploratory, investigation as well as analytical and information activities. The ABW may use, among others, operational control, controlled purchase, classified surveillance of consignments as well as the assistance of persons other than officials of the Agency.

921. Moreover, the Head of the ABW coordinates operational and exploratory activities undertaken by special services which may have an impact on the security of the state by keeping a central register of operational interests of the special services.

922. Pursuant to Articles 5 and 8 *of the Act of 10 June 2016 on counter-terrorist activities* , the Head of the ABW also coordinates operational, exploratory, analytical and information activities with regard to terrorist events carried out by special services, as well as the exchange of information in this respect provided by the Police, the Border Guard, the Marshal's Guard, the State Protection Service, the State Fire Service, the National Revenue Administration, the Military Police and the Government Security Centre.

923. In the structure of the ABW there are separate organisational units which are responsible for, inter alia, identifying, preventing and combating financing of terrorism (ABW Counter-Terrorist Centre) and the predicate offences in which money laundering may occur (the ABW Strategic Threats Department).

924. Within the framework of its activities, the ABW closely cooperates with domestic partners (special services, the Police, the Border Guard, the KAS, etc.) and foreign partners (bilaterally and on multilateral fora).

925. One of the main priorities of the KAS is to prevent and combat tax crime (including VAT crime), in particular through the systematic identification of threats, control activities, and the identification of specific persons and entities suspected of pursuing criminal activities. For this purpose, operational and exploratory activities are conducted. They are used in a wide range of cases concerning avoidance or understatement of taxes, including: irregularities in trade in excise goods (including tobacco products, spirits, fuels), VAT carousels, identification of so-called "blank invoices" documenting fictitious trade in various goods or services, irregularities related to intra-Community trade in goods and smuggling, illegal gambling, failure to record revenue in business activity, understatement of tax bases, fraudulent VAT evasion from the State Treasury.

926. Prosecution of crime revealed by the authorities of KAS under Article 299 of *the Penal Code*, in connection with which there has been a depletion or exposure to depletion of public law receivables, is a task imposed on KAS under the *Act of 24 November 2017 amending certain acts in order to prevent the use of the financial sector for tax fraud* (Journal of Laws of 2017 item 2491) which entered into force on 13 January 2018, amending the *Act of 16 November 2016 on the National Revenue Administration* (Journal of Laws of 2019 item 769 as amended).

927. In the years 2016-2018, many new organisational and legislative solutions were implemented supporting combating of economic crime. In order to tighten tax collection and counteract and combat economic crime, a number of new legal solutions have been introduced as part of the so-called fuel, transport, tobacco and spirits package. The rules of VAT registration and settlement were modified (including liquidation of quarterly settlements for specific groups of taxpayers, modification of the rules of VAT refunds, extension of the scope of application of the reverse charge mechanism, reinstatement of sanctions for unreliable VAT settlement), cash payments were reduced, new methods for the control of supply and purchase records (JPK) were introduced. In addition, the mechanism of joint and several liability was extended, more stringent fiscal penal sanctions for issuing invoices were introduced and extended confiscation was introduced. Among others, projects were implemented related to the introduction of the system of split VAT payment, the ICT system of the clearing house (STIR), which enables the analysis of the risk of using the activities of banks and cooperative savings and credit unions for purposes related to tax fraud.

928. The KAS is also responsible for the performance of the tasks arising from Article 3(4) of *Regulation (EU, EURATOM) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999* (OJ L 248, 18.09.2013, p. 1), i.e. the coordinating unit, in cooperation with the European Anti-Fraud Office (OLAF), combating financial abuse (Anti-Fraud Coordination Service - AFCOS).

929. The Undersecretary of State at the Ministry of Finance, being the Deputy Head of the KAS, acts as the Government Plenipotentiary for Combating Financial Irregularities to the detriment of Poland or the EU who is responsible in particular for the organisation of the process of reporting by Poland of irregularities in the use of EU funds, in accordance with the requirements determined by the European Commission.

930. One of the questions included in the questionnaires distributed in the second half of 2017 by the GIFI included a request to indicate an assessment of cooperation with other national authorities and units[453] dealing with preventing and combating fiscal crime and offences in terms of counteracting and combating offences that generate profits and money laundering on a four-stage scale (from 1 - very bad to 4 - very good). The average evaluation of cooperation with particular law enforcement agencies[454] indicated by respondents, representing law

[453] A list of the following authorities was indicated: the Police (without the CBŚP) , the CBŚP, the Border Guard, the ABW, the AW, the SWW, the SKW, the Military Police, prosecutor's office organisational units, the GIFI, tax control authorities, customs and tax control authorities, the KNF (PFSA), the NBP (to the extent it performs oversight functions in relation to entities conducting bureaux de change activity).
[454] i.e. without reference to the KNF (PFSA) and the NBP.

enforcement agencies[455] who answered this question, ranged from 3.2 to 4.0. The justifications for the evaluations indicated, inter alia, the need to apply appropriate investigation tactics, including the collection of evidence not only of the predicate offence but also of money laundering, shortening the time of tax inspections, facilitating the exchange of information via tele transmission or problems in accessing information covered by fiscal secrecy.

931. It is worth emphasising that Resolution No. 181 of the Council of Ministers of 6 October 2015 adopted the "Programme on counteracting and combating economic crime for the years 2015-2020"[456] Within the framework of the adopted action plan for the implementation of the above-mentioned programme, tasks related to counteracting money laundering and financing of terrorism are performed, i.e:

- strengthening the coordination of inter-institutional cooperation in the scope of counteracting money laundering;
- drafting a new regulation in relation to anti-money laundering issues in line with EU requirements[457];
- coordination of the implementation of evaluation conclusions in relation to the anti-money laundering system.

932. Another task provided for in the programme is to set up the register enhancing the security of the functioning of the financial market as regards information on bank accounts, insurance contracts with investment elements as well as other products for collecting, storing or investing fund and to provide access to it for law enforcement authorities and other relevant entities. Due to the fact that Directive 2018/843 commits EU Member States to establish a centralised automatic mechanism to enable the relatively rapid identification of any natural or legal person holding or controlling payment accounts and bank accounts and safe deposit boxes, the implementation of this task is linked with the implementation of the provisions of this Directive.

933. In connection with the adoption of the aforementioned resolution, Interministerial Team for Coordination of Implementation, Monitoring and Evaluation of the “Programme for Counteracting and Combating Economic Crime for the years 2015-2020” was established pursuant to Resolution No. 122 of the Prime Minister of 3 November 2015. It is chaired by the Minister of Internal Affairs and Administration or by his designated Secretary of State or Undersecretary of State at the Ministry of the Internal Affairs and Administration. The Team consists of:

- the Minister of Justice (or his designated Secretary of State or Under-Secretary of State at the Ministry of Justice);
- the minister competent for computerisation (or the secretary of state or undersecretary of state in the office servicing the minister competent computerisation, appointed by him);
- the minister competent for economy (or his designated secretary of state or undersecretary of state in the office servicing the minister competent for economy);

[455] Seven completed questionnaires were received, while this question was answered in 3 of them.
[456] Official Gazette of the Republic of Poland (Monitor Polski) of 2015, item 1069, as amended.
[457] This task was performed through designing and adopting of the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*.

- the minister competent for energy (or his designated secretary of state or undersecretary of state in the office servicing the minister competent for energy);
- Minister - Member of the Council of Ministers, Coordinator of Special Services (or a representative authorised by him);
- the Secretary of the College for Special Services or a representative authorised by him;
- the GIFI (or the Director of the Financial Information Department of the Ministry of Finance as his deputy);
- Head of the ABW (or his deputy);
- Head of the CBA (or his deputy);
- Head of the KAS (or his deputy);
- The Chief Commander of the Police (or his deputy);
- The Chief Commander of the Border Guard (or his deputy);
- The Chief Commander of the Military Police (or his deputy);
- The Chair of the KAS (or his deputy);
- Deputy General Prosecutor responsible for economic crime (or Director of the Department for Economic Crime at the National Prosecutor's Office as his deputy).

934. The tasks of the above mentioned Team comprise:

- assessing, adopting and updating schedules for the implementation of the tasks arising from the action plan of this programme;
- determining the manner of implementation of tasks resulting from the aforementioned action plan;
- monitoring the implementation of tasks resulting from the aforementioned action plan;
- annual evaluation of the status of implementation of the tasks in the aforementioned action plan.[458]

935. The exchange of criminal information is possible thanks to the KCIK, acting under the provisions of *the Act of 6 July 2001 on the processing of criminal information* (Journal of Laws of 2019 item 44 as amended). In accordance with this Act, criminal information shall include data concerning cases being the subject of operational and exploratory activities (the scope of such data is defined in Article 13(1) of this Act), initiated or completed criminal proceedings, including proceedings in cases of fiscal offences and related to other proceedings or activities carried out pursuant to the Acts by entities bound to submit them to the KCIK, relevant for operational and exploratory activities or criminal proceedings.

936. The entities authorised to obtain criminal information from the KICK (as defined in the aforementioned legal act) are:

---

458 https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/organy-pomocnicze/organy-pomocnicze-rady/3726,Miedzyresortowy-Zespol-do-spraw-koordynacji-wdrazania-monitorowania-i-ewaluacji-.html, date of reading 25 June 2019

- prosecution authorities;
- police authorities;
- the CBA;
- the ABW;
- bodies of the Border Guard;
- the Marshal's Guard;
- the authorities of the KAS, customs and tax control authorities;
- the State Protection Service;
- the Military Police;
- financial information authorities (in particular, the GIFI);
- public administration bodies competent in matters of citizenship, foreigners and repatriation;
- the Head of the Military Counter-Intelligence Service and the Head of the Military Intelligence Service;
- the Chair of the KNF (PFSA) or a representative authorised by him;
- the national administrator referred to in Article 3(22) of *Commission Regulation (EU) No 389/2013 of 2 May 2013 establishing a Union Registry pursuant to Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No 406/2009/EC of the European Parliament and of the Council and repealing Commission Regulations (EU) No 920/2010 and No 1193/2011* (OJ L 122, 03.05.2013, p. 1);
- Director General of the State Forests, directors of regional directorates of the State Forests, forest district governors and the Chief Inspector of the Forest Service;
- national park directors.

937. On the other hand, the entities obligated[459] to provide criminal information are authorised entities and:

- government administration bodies or local government bodies competent in matters of population records, the Universal Electronic System of Population Records, passport records, the Register of Personal Evidence, military records referred to in Article 49 of *the Act of 21 November 1967 on the universal obligation to defend the Republic of Poland* (Journal of Laws of 2018, item 1459, as amended), central register of vehicles, central register of drivers, vehicle registration, civil aircraft register, administrative register of Polish inland waterway vessels, Polish yacht register, Polish

[459] Pursuant to Article 24 of *the Act of 6 July 2001 on the processing of criminal information*, the obligated entities may refrain from submitting criminal information to the Head of the KCIK or limit the scope of the information submitted if its submission could endanger the security of the State or its defence or cause the identification of persons providing assistance in the performance of operational and exploratory activities carried out by authorised entities. However, they shall provide it as soon as the reason for the failure to transmit or the restriction of the scope of criminal information transmitted ceases to exist.

ship register, surveying and cartographic surveillance, land and building register, registration of civil status, public employment or social assistance service;

- courts maintaining the National Court Register, Land and Mortgage Registers and the Pledge Register;
- Environmental Protection Inspection authorities;
- State Fire Service authorities;
- Social Security Institution authorities;
- President of the Agricultural Social Insurance Fund;
- Polish Financial Supervision Authority;
- State Fishing Service;
- President of the Office for Competition and Consumer Protection;
- President of the Central Statistical Office and directors of the statistical offices as regards national official registers maintained by them;
- director of the Information Office of the National Criminal Register;
- directors of the Prison Service organisational units;
- State Hunting Service.

938. Entities authorised are obliged to provide the Head of the KCIK with criminal information ex officio. Its scope comprises the following areas:

- crime and offences,
- persons against whom criminal proceedings are conducted, including proceedings for fiscal offences, or in relation to whom operational and exploratory activities are conducted (hereinafter referred to as "persons"),
- objects used to commit the offence or lost in connection with the offence (hereinafter referred to as “objects”),
- entrepreneurs, civil partnerships, foundations, associations reasonably suspected of having been used to commit a criminal offence (hereinafter referred to as “entities”),
- numbers of bank accounts or securities accounts in relation to which there is a reasonable suspicion that they have been used for the purpose of committing an offence or that the proceeds of crime are collected thereon (hereinafter referred to as “accounts”) .

939. Obligated entities, other than authorised entities, provide criminal information to the Head of the KCIK only on his request.

940. As of 31 December 2018, 30,419,891 pieces of criminal information were collected in the KCIK databases, submitted to the Centre pursuant to Article 21(1) of the aforementioned Act, including 1,764,538 pieces of information sent in 2018.[460]

[460] Report on the activities of the National Centre for Criminal Information for 2018, Head of the KCIK - Chief Commander of the Police, Warsaw, March 2019, p. 6.

941. In 2018, the authorised entities submitted 172,070 requests for information to the KCIK database. Among these, approx. 22.8% additionally included an order to supplement information based on data collected by obligated entities. Since the authorised entities indicated one or more authorities as sources of additional information, the KCIK has developed and transmitted to the authorised entities 139,792 requests in this scope.[461]

942. In addition, in 2018, 335,878 pieces of coordination information were generated and sent in the IT system of the KCIK (addressed to the owner of the criminal information and concerning the transmission of the criminal information obtained from the owner to the authorised entity).[462]

943. Other questions included in the questionnaires distributed in the second half of 2017 by the GIFI related to indication of an assessment of cooperation with other entities/units[463] in the scope of counteracting and combating terrorism and its financing on a four-stage scale (from 1 - very bad to 4 - very good). The respondents, representing law enforcement agencies[464]who answered this question, evaluated this cooperation at level 4.

944. It is worth emphasising that in Poland the Inter-ministerial Team for Terrorist Threats, mentioned in subchapter 6.1 operates. It was established pursuant to Regulation No 162 of the Prime Minister of 25 October 2006.[465] The basic assignments of the Team include, inter alia: monitoring of terrorist threats, presenting opinions and conclusions to the Council of Ministers, developing draft standards and procedures in the scope of combating terrorism, initiating and coordinating activities undertaken by the competent governmental administration bodies, organising cooperation with other countries in the scope of combating terrorism, etc. The Team is chaired by the Minister of Internal Affairs and Administration[466]. It is composed of (excluding the secretary indicated by the chairman):

- the minister competent for public finance (as deputy chairman);
- the minister competent for financial institutions (as deputy chairman);
- Minister of National Defence (as deputy chairman);
- the minister competent for foreign affairs (as deputy chairman);
- Minister of Justice (as deputy chairman);
- Minister - Member of the Council of Ministers, Coordinator of Special Services (as deputy chairman);
- secretary of state or undersecretary of state appointed by the minister competent for internal affairs, supervising the conduct of cases covered by the department of

[461]Ibidem, p. 24.
[462]Ibidem, p. 40.
[463] A list of the following authorities was indicated: the Police (without the CBŚP) , the CBŚP, the Border Guard, the ABW, the AW, the SWW, the SKW, the Military Police, prosecutor's office organisational units, the GIFI, tax control authorities, customs and tax control authorities, the KNF (PFSA), the NBP (to the extent it performs oversight functions in relation to entities conducting bureaux de change activity).
[464] Seven completed questionnaires were received, while this question was answered in 3 of them.
[465]https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/organy-pomocnicze/organy-pomocnicze-rady/128,Miedzyresortowy-Zespol-do-Spraw-Zagrozen-Terrorystycznych.html, date of reading 25 June 2019
[466] The function of the Chairman of the Team may be performed, on behalf of the Minister of Internal Affairs and Administration, by a secretary or undersecretary of state at the Ministry of Internal Affairs and Administration authorised by him.

governmental administration - internal affairs in the field of security and public order protection;

- secretary of state or undersecretary of state appointed by the minister competent for internal affairs, supervising the conduct of cases covered by the department of governmental administration - internal affairs in the field of in crisis management, fire protection and civil defence;
- The Secretary of the College for Special Services (or his deputy);
- Head of National Civil Defence (or his deputy);
- Director of the Government Security Centre (or his deputy);
- Head of the ABW (or his deputy);
- Head of the AW (or his deputy);
- Commander of the State Protection Service (or his deputy);
- Chief Commander of the Police (or his deputy);
- Chief Commander of the Border Guard (or his deputy);
- Chief Commander of the State Fire Service (or his deputy);
- Chief of General Staff of the Polish Army (or his deputy);
- Operational Commander of the Types of Armed Forces (or his deputy);
- Head of the Military Intelligence Service (or his deputy);
- Head of the Military Counterintelligence Service (or his deputy);
- Chief Commander of the Military Police (or his deputy);
- Head of the KAS (or his deputy);
- the GIFI (or his deputy).

945. Another question from the aforementioned surveys concerned cooperation at the international level. When asked to provide an assessment of cooperation in preventing and combating profit-generating crimes and money laundering with their counterparts abroad on a four-stage scale (from 1 - very bad to 4 - very good), respondents rated the cooperation with authorities from other EU Member States on an average level of 3.7 and with authorities from non-EU countries - on an average level of 2.6. While indicating the areas that need improvement, the following aspects were listed, among others:

- the time taken to process requests for legal aid;
- full implementation of the activities listed in the requests for legal aid;
- prolonged response time (in the case of cooperation with non-EU countries);
- rapid communication of potential deficiencies in requests for legal aid preventing their implementation (in case of cooperation with non-EU countries);
- facilitating access to data.

946. The respondents also evaluated the cooperation in this area with international bodies and organisations cooperating on the basis of agreements other than bilateral ones. The average of

their evaluation was 3.3. Among the areas that need improvement, the need to develop electronic information exchange channels and Internet access portals was indicated.

947. Questions asking for an indication of an assessment of cooperation in preventing and combating terrorism and its financing with their counterparts abroad on a four-stage scale (from 1 - very bad to 4 - very good) were answered, indicating an average rating of 3.5 both for cooperation with the authorities from other EU Member States and non-EU countries, as well as with international bodies and organisations cooperating under non-bilateral agreements.

7.3.4. Activities of the judicial authorities

948. The judiciary system in Poland is governed by the Supreme Court, common courts, administrative courts and military courts. Criminal proceedings concerning the suspicion of money laundering or financing of terrorism are conducted by common courts.

949. Below, verified data on criminal court proceedings conducted in 2017-2018 concerning suspected money laundering and financing of terrorism are presented.

Table No. 27 - Verified information concerning criminal proceedings conducted before the courts in the years 2017-2018[467]

year		2017		2018	
type of offence		**Article 165 of kk**	**Article 299 of kk**	**Article 165 of kk**	**Article 299 of kk**
Number of instituted criminal proceedings		1	175	-	158
number of persons against whom proceedings have been initiated		3	463	-	401
assets (in PLN) in relation to which:	**account blocking or transaction suspension was performed**	-	304,740	-	2,032,243
	seizure was ordered	-	250,000	-	396,092
	proprietary security was applied	-	792,809	-	1,357,198,213
	forfeiture was declared	-	166,376,609	-	124,997,528
Adults, convicted:	**In the 1st instance**	3	424	-	323
	Finally	-	262	3	228

950. In 2018, in terms of the number of instituted criminal proceedings concerning offences under Article 299 of *the Penal Code* as well as the number of persons convicted in the first instance with a legally binding verdict, a certain decrease can be observed in relation to the data for 2017 (by 9.7%, 23.8% and 13.0% respectively). It is worth noting, however, that these figures are higher than those recorded in previous years. For example, according to information from the Ministry of Justice published in the annual reports of the GIFI, in 2016 common courts instituted 113 criminal proceedings for offences under Article 299 of *the Penal Code*, and in 2015 - 127[468] In 2015, 311 persons were sentenced for committing the above mentioned crime (verdicts not final) and 151 persons were finally sentenced (and according to data from the National Prosecutor's Office, in 2016 there were 100 verdicts concerning 251 persons in total).

951. An estimation of the data performed in order to provide input to the update of the transnational risk assessment of money laundering and financing of terrorism shows that the average length of criminal proceedings in 2017 between the formulation of the indictment and issuing of the first instance verdict was about 5.1 - 5.5 months.

[467] Based on information provided by the Ministry of Justice on 25 March 2019.
[468] Report of the General Inspector of Financial Information on the implementation of the *Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2016, Warsaw, 2017 p. 23; Report of the General Inspector of Financial Information on the implementation of *the Act of 16 November 2000 on counteracting money laundering and terrorist financing* in 2015, Warsaw 2016, p. 21.

8. SUMMARY OF THE NATIONAL ASSESSMENT OF THE RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM

8.1. MONEY LAUNDERING RISK ASSESSMENT

8.1.1. Assessment of primary risk

Level of threat

953. In accordance with the methodology set out in Annex 1, the calculation of the level of money laundering risk for the basic risk assessment should be based on an estimation of the assets coming from illegal activities, an assessment of the threat of Poland with the profit-generating crime, the level of risk of money laundering in the EU indicated in the supranational risk assessment of money laundering and financing of terrorism, as well as possible information concerning Poland originating from money laundering and financing of terrorism risk assessments of other countries.

954. There are not sufficiently reliable data to estimate with certainty the profits from illegal activities that may be subject to laundering. On the other hand, taking as a starting point the estimates presented in chapter 5.2. concerning possible profits from illegal activities which for 2017 range from 1.08% of GDP to about 1.27% of GDP (and for 2018, the lower limit of this range can be estimated at about 1.04% of GDP), it can be indicated with a high degree of probability that they may have exceeded 1% of GDP in recent years. It is worth noting, however, that according to IPAG estimates, the share of the shadow economy (and thus illegal activity) in the Polish economy has been steadily decreasing since 2015, also in 2019 it is expected to be smaller than in the previous year. According to the Institute, the reasons for this are the actions taken by the authorities to tighten the tax system as well as the effective fight against illegal activities (including the reduction of production and trade in drugs and designer drugs, cigarette smuggling and the elimination of illegal gambling).[469]

955. According to the Police data, the detection of crime increases year by year. In 2017, it amounted to 71.7% (more than in the previous two years), with the highest rate of detection of offences *under the Act on counteracting drug addiction* (76.7%), economic crime (87.6%) and crime related to robbery, theft and extortion (73.6%).

Table no. 28 - Police data on offences found, detected and their detection rate in the years 2015-2017[470]

[469] Jacek Fundowicz, Krzysztof Łapiński, Bohdan Wyżnikiewicz, Dorota Wyżnikiewicz, Shadow economy 2019, IPAG, Warsaw, March 2019, p. 24, available at: www.ipag.org.pl/Content/Uploaded/files/IPAG_Szara_Strefa_2019.pdf.
[470] According to data available on: http://statystyka.policja.pl/st/wybrane-statystyki , date of reading 11 June 2019

data category	offences in general	selected categories of offences				
		economic crime	offences *under the Act on counteracting drug addiction*	robbery, theft and extortion	burglary	stealing someone else's items
2017						
% of detection	71.7%	87.6%	96.7%	73.6%	36.5%	32.0%
offences found	753,963[471]	189,871	55,638	6,053	65,514	108,248
offences detected	545,008	166,776	53,821	4,517	24,746	35,359
2016						
% of detection	66.5%	82.5%	96.1%	69.2%	34.5%	29.6%
offences found	748,459	150,386	51,323	7,444	77,190	127,801
offences detected	501,877	124,444	49,313	5,204	27,535	38,528
2015						
% of detection	64.7%	84.4%	96.0%	63.8%	31.6%	28.1%
offences found	799,779	167,741	46,431	7,787	91,328	145,464
offences detected	524,380	142,124	44,563	5,055	30,256	42,046

956. According to the CBA report "Combating corruption crime in Poland in 2017 in 2017", 36,247 corruption offences were registered in the KCIK, i.e. over 28% more than in the previous year[472] About 97.0% of these offences were registered by the Police, the remaining ones were indicated by the prosecutor's office, the CBA, the SG, the ŻW and the ABW. Also, most preparatory proceedings in corruption cases in 2017 were initiated by the Police[473]

957. The information on the activities of the KAS shows that in 2018 (in comparison with data for 2017) the number of instituted preparatory proceedings in cases concerning fiscal penal offence decreased by approx. 31.2%, including the number of preparatory proceedings in cases concerning fiscal offences - by approx. 25.4% and the number of cases concerning fiscal offences by 33%. This decline was related to systematic measures carried out at the Ministry of Finance, aimed at tightening the tax system, which contributed to reducing the scale of irregularities in this area. In addition, the smaller scale of tax crime resulted mainly from the effectiveness of the activities of the KAS in combating and counteracting tax and customs fraud.

958. In accordance with the Police information, in 2018 795,976 offences were committed and their detection rate increased to about 74.1%[474] At the same time, a decrease in the number of offences committed was noted, inter alia, in such categories as: robbery, extortion and theft, property theft, car theft, economic crime and corruption offences.

959. It is worth noting, however, that according to the information provided by the CBŚP, the number of organised criminal groups of interest to the Bureau has increased (from 742 in 2017 to 880 in 2018), as well as the number of persons active in them (from 7,113 in 2017 to 8,030

[471] According to updated information, 765,176 offences were committed in 2017, excluding maintenance offence -http://policja.pl/pol/aktualnosci/168195,Mniej-przestepstw-kryminalnych-wieksza-skutecznosc-i-wykrywalnosc-Policja-podsum.htmldate of reading 21 June 2019.

[472]Combating corruption crime in Poland in 2017, CBA, Warsaw 2019, p. 7, available at: http://antykorupcja.gov.pl/ak/wydawnictwa-cba/13380,Zwalczanie-przestepczosci-korupcyjnej-w-Polsce-w-2017-r.html.

[473]Ibidem, p. 13.

[474]http://policja.pl/pol/aktualnosci/168195,Mniej-przestepstw-kryminalnych-wieksza-skutecznosc-i-wykrywalnosc-Policja-podsum.html , date of reading 21 June 2019

in 2018)[475] This may indicate that the threat stemming from the offences committed by these groups is not decreasing.

960. At the same time, the CBŚP demonstrated that in 2018, in total 391 firearm pieces were seized (in 2017 - 363 pcs.), including: short weapons - 169 (in 2017 - 143 pcs.), long weapons - 86 (in 2017 - 73 pcs.), gas weapons - 110 (in 2017 - 17 pcs.) and other (i.e. machine guns, signal guns, alarm guns, self-propelled guns, gunshells) - 26 pcs. (in 2017 - 130 pcs.)[476] It was still less than in 2016, when the CBŚP seized a total of 552 firearms pcs.[477]

961. The "Report on the state of security in Poland in 2016" indicates that the armed conflict in Ukraine and the permanent, intensified terrorist threat have resulted in an increase in demand for goods, technologies and services of strategic importance to state security, i.e.: arms, ammunition, explosives, uniforms (including: bulletproof vests), protective equipment, heavy equipment that can be used for military purposes. At the same time, criminal groups are increasingly trying to organise channels for smuggling weapons and ammunition from the territory of Ukraine to the Republic of Poland and further into the EU[478]

962. The risk of crime is still high, although due to increasing detectability as well as the efforts made to reduce fiscal crime, which until now has been identified as one of the main categories of crime from which the laundered assets originated, the risk of predicate offences for money laundering can be assessed between medium and high.

963. The European Commission transnational assessment of the risk of money laundering and financing of terrorism published in June 2017, did not identify the overall level of risk of money laundering for the EU[479] On the other hand, it identified 40 products and services in 11 areas that are potentially vulnerable to money laundering and financing of terrorism and for which it identified levels of threat and vulnerability (separately for money laundering and separately for financing of terrorism). At the same time, it pointed out that, in general, the EU internal market remains vulnerable to the risk of money laundering and financing of terrorism, with criminals using increasingly complex methods and taking advantage of the new opportunities generated by the emergence of new types of products and services[480] It can therefore be assumed that the risk of money laundering in the EU is at least moderate (medium) if not high[481]

---

[475] Report on the activities of the Central Investigation Bureau of the Police for 2018 (in statistical terms), CBŚP, Warsaw 2018, p. 2, available at: http://www.cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

[476] Ibidem, p. 9.

[477] Report on the activities of the Central Investigation Bureau of the Police for 2018 (in statistical terms), CBŚP, Warsaw 2018, p. 8, available at: http://www.cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

[478] Report on the state of security in Poland in 2016, MSWiA, published in October 2017, p. 118, available at: https://archiwumbip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html

[479] Until 18 June 2019, the European Commission has not yet published an update of the transnational assessment of the risk of money laundering and terrorist financing. In accordance with Article 6(1) of Directive 2015/849, the aforementioned assessment must be updated at least once in two years.

[480] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 26 June 2017, p. 20, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

[481] If one were to rely only on the assessments of threat and vulnerability to money laundering assigned to 40 products and services assessed by the European Commission, the average level of threat to money laundering would be about 2.7 on a four-level scale and the average level of vulnerability to money laundering would be about

964. Information available on the content of other countries' national assessments of money laundering and financing of terrorism shows that Poland has sporadically been identified as one of the main countries from which illegal assets originate or to which they are transferred.

965. In the national assessment of money laundering and financing of terrorism for Latvia of 2018, it was mentioned (while referring to the analysis of financial flows - without classifying them as suspicious) that Poland was one of the 5 main countries (along with Lithuania, Germany, Russia and Estonia) to which Latvian funds are transferred.[482] At the same time, Poland was also mentioned in the context of the activities of international criminal groups specialising in money laundering as one of the countries of origin of such groups[483]. It was also noted that companies registered, among others, in Poland are used for tax avoidance purposes by Latvian citizens, although at the same time a trend of migration of this illegal activity to other countries was observed.[484] It was found that Poland generates the threat of money laundering for Latvia at a medium-high level (i.e., at level 4 on a five-level scale), although a downward trend in this respect was also noted. It was indicated that the largest amounts of confiscated assets came from 3 countries, including Poland.

966. On the other hand, in the national risk assessment of Slovakia referring to the analysed cases of money laundering, it was found that although in the vast majority of them Slovakia was the target country, in the remaining cases 3 other countries, including Poland were indicated as the target countries (about 1.03% of cases).[485]

967. In some national assessments of the risk of money laundering and financing of terrorism of other countries, reference can also be found to Poland in the examples given of money laundering cases or in relation to the threat of predicate offences for money laundering.

968. Based on the above information, it is possible to determine the level of money laundering risk in Poland, in particular with respect to the estimates of profits from illegal income and the risk of predicate offence for money laundering, at least at a high level (i.e. at level 3 on a four-level scale).

Level of vulnerability

969. In accordance with information presented in subchapter 7.1. there are few types of products and services offered in Poland that can directly facilitate performing fast and anonymous transactions. In recent years, public administration bodies have made great efforts to communicate and mitigate the risks associated with them in the broadest possible way (e.g. by covering entities offering virtual currency services with anti-money laundering and counter-financing of terrorism obligations or by specifying rules for offering prepaid cards). It is also worth noting the relatively low share of cash transactions among transactions above EUR 15 thousand.

2.6 on a four-level scale, indicating a level of risk between medium and high levels (i.e. between 2 and 3 on a four-level scale).

[482] Supplemented Latvian National money laundering/terrorism financing risk assessment report, Riga, 22 June 2018, p. 41, available at: http://www.kd.gov.lv/index.php/en/useful/national-risk-assessment.

[483]Ibidem, p. 34.

[484]Ibidem, p. 42.

[485] Final report on the national assessment of the risk of money laundering and terrorist financing in the conditions of the Slovak Republic, p. 12 and 57, available at: https://www.minv.sk/swift_data/source/policia/fsj/mv/ANNEX34.pdf.

970. In today's globalised world, financial flows between different jurisdictions are more and more frequent. The execution of transactions from Poland to another country is not difficult. It is worth noting, however, that although most transactions, including those of an international nature, are carried out through banks, they are at the same time the category of obligated institutions which regularly provide the vast majority of information on suspicious transactions and activities to the GIFI.

971. The catalogue of obligated institutions, indicated in Article 2(1) of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, contains most of the entities which - due to the products or services offered and the analysis of threats to money laundering or financing of terrorism - should fulfil the obligations to prevent these crimes, including applying customer due diligence measures and cooperating with the GIFI. However, there are also some entities that remain outside this catalogue, despite the risks associated with their activities (in particular, those identified in the transnational risk assessment or in Directive 2018/843).

972. Those entities which are obligated institutions generally have knowledge of their obligations in relation to money laundering and financing of terrorism.

973. During inspections carried out by the GIFI as well as other authorities and entities indicated in Article 130(2)(1) of the aforementioned Act, there are also relatively frequent cases of irregularities in the scope of fulfilling the obligations resulting from the provisions on counteracting money laundering and financing of terrorism by the obligated institutions. Although it must be remembered that their type and weight does not always require an administrative procedure to impose a penalty.

974. Public administration authorities involved in the national anti-money laundering system, in particular the supervisory authorities of different categories of institutions, the GIFI as well as law enforcement agencies have adequate knowledge of the risks of money laundering and financing of terrorism. This is evidenced, among other things, by various statements, reports and information on individual cases published by these bodies.

975. The information available indicates that in most cases the supervision authorities of the obligated institutions have adequate resources to carry out control over those entities. All supervision authorities communicate information on the inspections carried out to the GIFI and the results of the inspections performed give rise to imposing of administrative sanctions and the application of other supervisory instruments in relation to obligated institutions. In accordance with the provisions of *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the GIFI takes measures to coordinate control activities by other supervision authorities. Cooperation of the GIFI and the UKNF (PFSA office) with their foreign counterparts is at a high level.

976. The GIFI is well aware of the risk of money laundering and financing of terrorism. Moreover, it has a relatively good ability to collect and analyse information on suspicious activities and transactions, i.e.:

- it has direct or indirect access to most public administration databases needed to analyse information on suspicious activities and transactions;
- it is entitled to receive additional information from the obligated institutions and cooperating units on request;

- newly hired analysts at the Financial Information Department of the Ministry of Finance undergo practical training in the scope of conducting analyses (in the unit dealing with preliminary analysis of information on suspicious transactions and activities).

977. Over the last few years, the number of employees of the Financial Information Department of the Ministry of Finance has been slowly increasing, to reach 75 at the end of May 2019. However, the assessment of the potential for the implementation of the tasks imposed on the above mentioned unit shows that their higher number is required. The activities of the Department are sufficiently financed within the budget of the Ministry of Finance.

978. The GIFI also has its own IT system enabling receiving, collecting and analysing information on suspicious activities and transactions.

979. The exchange of information between the GIFI and other cooperating units, in particular law enforcement agencies, is relatively smooth, especially as regards the provision of information by the GIFI on request (they are not limited by the scope and type of data and the type of the law enforcement agency or judicial authority[486], the replies of the GIFI were provided in 2018 on average within 11 days, although a large part of them was sent on the same day as the request was received). However, it is reasonable to develop an ICT system for the exchange of information (primarily with all law enforcement agencies) as well as to develop templates for electronic documents, which should facilitate and speed up the transmission of requests and answers.

980. The international cooperation of the GIFI, in particular the exchange of information with its foreign counterparts, is relatively good. The currently effective legislation does not restrict the GIFI in the scope and type of data transmitted. Responses to requests for information from abroad are also provided in a relatively short period of time (in 2018,on average about 12 days, in the case of a large part of requests - more than ¼ of their number - replies were sent within 2 days). Information exchange is carried out through 2 ICT systems dedicated to this task, i.e. ESW (in the scope of cooperation with non-EU FIUs) and FIU.NET (for cooperation with EU FIUs).

981. In Poland, there are 3 fora where issues related to counteracting and combating money laundering, financing of terrorism and predicate offences for money laundering are analysed and discussed. The first one is the Financial Security Committee, operating under the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism.* The next ones include the Interministerial Team for coordinating the implementation, monitoring and evaluation of the "Programme for Counteracting and Combating Economic Crime for 2015-2020" and the Interministerial Team for Terrorist Threats. Their members include the GIFI and representatives of law enforcement agencies as well as other public administration bodies. The above mentioned committees meet regularly.

982. In terms of information exchange at the national level, an important role is played by the KCIK, where criminal information is collected and through which additional information can be obtained from other entities bound to submit information to the KCIK.

[486] It should be remembered that only judicial authorities conducting criminal proceedings are taken into account.

983. In accordance with the information available, cooperation between law enforcement agencies and their foreign counterparts and international crime combating organisations has a good level (answers provided by law enforcement agencies are not likely to be limited by the scope and type of data and their considerable part uses electronic communication channels to exchange information quickly and securely with their foreign counterparts - in particular in the case of cooperation within the EU). Similar situation occurs in the case of national cooperation between individual law enforcement agencies.

984. The National School of the Judiciary and the Public Prosecutor's Office provides a number of training courses for judges, court staff and public prosecutors, including those concerning predicate offence for money laundering, asset security and forfeiture. It also provides information on international training in the scope of combating terrorism and its financing[487]

985. Data concerning criminal proceedings conducted before courts in cases concerning crime under Article 299 of *the Penal Code* indicate that in relation to 2017, the number of the above-mentioned criminal proceedings instituted in 2018 decreased by approx. 9.7%, the number of persons sentenced in the first instance by legally binding verdicts has also decreased - by 23.8% and 13.0% respectively.

986. However, it is worth noting the relatively short average length of criminal proceedings. In accordance with the data for 2017 - from the formulation of the indictment to the delivery of the verdict in the first instance - it amounted to approx. 5.1 - 5.5 months, i.e. less than six months.

987. The current anti-money laundering and counter-terrorist financing legislation largely corresponds to the extent of the risk of money laundering and financing of terrorism as well as EU legislation and the FATF recommendations. Currently, in 2019, works are carried out with the aim to implement the entire Directive 2018/843 as well as to complete the implementation of several provisions of Directive 2015/849.

988. Although the European Commission, in its "additional reasoned opinion" on the lack of notification of measures transposing Directive 2015/849 into the national law, indicated relatively numerous deficiencies in the implementation of the above-mentioned EU legal act, after its analysis, the national authorities concluded that in the vast majority of cases the provisions of the above mentioned Directive have been correctly transposed into national law.

989. It should be emphasised that the analysis performed in 2018 by the MONEYVAL Secretariat, in connection with the preparation of the Polish report under step 1 of the compliance enforcement procedure, includes a statement that *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* eliminates most of the deficiencies found within the fourth round of mutual evaluation.

990. In conclusion, the vulnerability in the area of money laundering (as well as financing of terrorism)[488] in the scope of underlying risk can be estimated at an average level.

[487] https://szkolenia.kssip.gov.pl/course/coursesearch/simplesearch.php , date of reading 26 June 2019

[488] In accordance with the methodology adopted, presented in Annex no. 1, the level of vulnerability to terrorist financing for the assessment of the underlying risk is to be based on the same elements as for the estimation of the level of vulnerability to money laundering for the assessment of the underlying risk.

Level of consequence

991. According to the Police data concerning the total number of detected offences, in 2017 and 2018 their numbers increased slightly, although at the same time their detectability improved. It was emphasised that the increase was mainly caused by a higher number of non-maintenance offences (in 2018 in relation to 2017, it increased by about 317%), which resulted from the amendments to criminal regulations in this area. Without taking into account this type of crime, the total number of remaining offences decreased by about 5.2% in 2018[489]

992. In accordance with the CBOS survey, published in 2018, about 86% of Poles expressed the belief that it is safe to live in Poland (i.e. 3 percentage points less than in 2017), while every ninth respondent (11%, i.e. 2 percentage points more than in the previous year) indicated that it is not safe to live in Poland[490] Most of the respondents, i.e. about 60%, did not feel the threat of crime. On the other hand, approx. 4% of respondents indicated their high fear of becoming a victim of crime and about 34% said they were afraid of it, but not so much[491]. According to press information, the latest CBOS survey conducted in 2019, indicates that the sense of security of Poles has increased (about 89% of Poles believe that living in Poland is safe, and the share of negative answers was about 8%)[492]

993. As noted at the beginning of this chapter, the estimates and forecasts presented by IPAG show that the share of the shadow economy (and thus illegal activity) in the Polish economy has been steadily decreasing since 2015 and is expected to be lower in 2019 than in 2018. However, in absolute figures, the value of the shadow economy is increasing (in 2019 it is expected to amount to about PLN 424 billion). According to IPAG's forecast, in 2019 alone, a total increase of PLN 19 billion in value added in the shadow economy will occur[493]

994. It should be assumed that the need to ensure an adequate number of staff and officers of public authorities and bodies (e.g. financial intelligence units[494]) will be associated with some increase in the operating costs of these bodies. Additional costs are incurred for the provision of appropriate equipment and technical infrastructure, including ICT.

995. It is worth noting that, at the same time, activities undertaken in the field of e.g. combating tax offences, considered to be one of the main types of predicate offences for money laundering, contribute to increasing the state budget revenues, in particular by reducing the so-called VAT gap[495].

[489] http://policja.pl/pol/aktualnosci/168195,Mniej-przestepstw-kryminalnych-wieksza-skutecznosc-i-wykrywalnosc-Policja-podsum.html , date of reading 21 June 2019

[490] Sense of security and crime threats, Survey Communication, No. 61/2018, CBOS, May 2018, p. 1.

[491] Ibidem, p. 3.

[492] https://forsal.pl/artykuly/1414931,cbos-89-proc-polakow-uwaza-ze-w-polsce-zyje-sie-bezpiecznie.html , date of reading 21 June 2019

[493] Jacek Fundowicz, Krzysztof Łapiński, Marcin Peterlik, Bohdan Wyżnikiewicz, Shadow economy, 2019, IPAG, Warsaw, March 2019, p. 24, available at: www.ipag.org.pl/Content/Uploaded/files/IPAG_Szara_Strefa_2019.pdf.

[494] In the Regulatory Impact Assessment attached at the turn of 2017 and 2018 to the then draft of the current *Act of 1 March 2018 on counteracting money laundering and terrorist financing*, it was predicted that employing additional people at the Ministry of Finance would cost about PLN 37.93 million for the next 10 years (counting from 2018).

[495] According to the estimates of the Ministry of Finance, in 2017, the so-called VAT gap amounted to 14% of the amount of theoretical VAT and about 1.3% of GDP (in 2016 it was estimated at 20% of the amount of theoretical VAT and 1.8% of GDP) - Tomasz Mazur, Dorota Bach, Agnieszka Juźwik, Iwona Czechowicz and Jadwiga Bieńkowska, Report on the size of the VAT gap in Poland in the years 2004-2017, MF Studies and Analyses, no.

996. It has not been found that Poland's credibility on the international arena has decreased due to the level of crime or the functioning of the anti-money laundering and counter-terrorist financing system. However, at least one report from another country's national assessment of the risk of money laundering and financing of terrorism states that Poland generates a money laundering threat at a medium-high level (i.e. at level 4 on a five-stage scale) and companies registered, among others, in Poland are used for tax avoidance purposes by citizens of this country.[496]

997. Summing up, the underlying risk implications of money laundering can be estimated at a low level (i.e., defining them as weak consequences), albeit with an upward trend to a moderate level (mainly due to references to Poland in the Latvian national assessment of money laundering risk).

Underlying risk estimation

998. In accordance with the methodology presented in Annex 1, the estimate of the underlying risk in the area of money laundering should be calculated using a formula: $R_{rp}=60\%*P_{rp}+40\%*K_{rp}$[497], where P_{rp} = $40\%*Z_{rp}+60\%*P_{rp}$[498]. Based on the last formula, the probability level of money laundering for the assessment of underlying risk, i.e. P_{rp} is 2.4, which is an average level. On the other hand, in accordance with the first formula, the underlying risk of money laundering is 1.84 and it is at an average level.

8.1.2. Assessment of residual risk

999. Annex 2 presents money laundering risk scenarios, compiled on the basis of both domestic and foreign experience in the scope of counteracting money laundering. They refer to the possibility of using various products and services offered both on and off the financial market to commit the above-mentioned crime. They are divided into areas where products and services are available.

1000. The level of vulnerability and threat was estimated for each of them, presented in Table 29.

Table No. 29 - Vulnerability, threat and probability levels for individual money laundering risk scenarios

Area	Risk description	Level of vulnerability	Level of threat	Level of probability[499]
Banking	using the account to collect and transfer money from illegal sources	2	4	2.8

3/2019, p. 20, available at: https://www.gov.pl/documents/1079560/1080340/No_3-2019_TMazur.pdf/437aa4f4-d590-4109-55ff-8ff1fd9ccba0.

[496] Supplemented Latvian National money laundering/terrorism financing risk assessment report, Riga, 22 June 2018, p. 42, available at: http://www.kd.gov.lv/index.php/en/useful/national-risk-assessment.

[497]where: R_{rp} - level of "underlying risk", P_{rp} - level of money laundering probability to assess "underlying risk", K_{rp} - level of money laundering consequences to assess "underlying risk".

[498]where: Z_{rp} - Money laundering threat level to assess the "underlying risk", P_{rp} - Money laundering vulnerability level to assess the "underlying risk".

[499] Calculated in accordance with the formula presented in Annex 1, i.e: $P_{ps}=40\%*Z_{ps}+60\%*P_{ps}$; where: P_{ps} - probability level for the scenario, Z_{ps} - threat level for the scenario, P_{ps} - vulnerability level for the scenario.

	acquiring credits and loans and repaying them with funds from illegal sources	2	3	2.4
	use of anonymous prepaid cards to hinder identification of money laundering perpetrators	2	1	1.6
	use of transfers in order to transfer funds to other jurisdictions	2	4	2.8
Payment services (offered by entities other than banks)	using cash transfer service providers to transfer money originating from illegal sources	2	4	2.8
	use of online payment services by perpetrators to transfer funds originating from illegal activities	3	3	3.0
	use of the Hawala network or other informal transfer systems to transfer funds originating from illegal sources	4	1	2.8
Insurance	taking advantage of the possibilities offered by unit-linked life insurance	2	2	2
Other financial institutions	using a brokerage company operating on the FOREX market as a "market marker" to legitimise funds originating from illegal sources	2	2	2
	purchase of participation units in investment funds for funds originating from illegal sources	2	2	2
	use of securities accounts and cash accounts to handle them in order to transfer and legitimise funds from illegal sources	2	3	2.4
Currency exchange	exchange of (cash) currency in order to make it difficult to identify money originating from crime	2	3	2.4
	exchange of low-denomination money to higher value banknotes	2	3	2.4
	cashless currency exchange combined with the transfer of funds	3	4	3.4
Virtual currencies	use of cryptocurrencies to transfer values from illegal sources	3	3	3.0
	use of centralised virtual currencies to transfer values coming from illegal sources	3	2	2.6
Telecommunication services linked with mobile payments	use of telecommunication services in the field of enhanced payment numbers to legitimise funds from criminal activity	4	2	3.2
Physical carriage of property values across borders	use of natural persons to transport money coming from illegal sources across state borders	4	4	4

	use of courier and postal services to transfer money coming from illegal sources	3	3	3
Gambling	funds coming from illegal sources are laundered through online gambling	2	2	2
	use of betting to legitimise funds coming from illegal sources	2	3	2.4
	use of casino games to obscure the origin of the money held	2	4	2.8
	buying the winning coupons for funds coming from illegal sources	2	2	2
Non-profit organisations	use of foundations and associations for money laundering	3	3	3
Crowdfunding	organising *crowdfunding* actions in order to legitimise the funds held or transferred	4	2	3.2
Trading in high value goods	investing funds coming from illegal sources in the purchase of metals and precious stones	3	3	3
	investing funds coming from illegal sources in the purchase of antiques and pieces of arts	3	2	2.6
Real estate trade	investing funds coming from illegal sources in real estate	2	3	2.4
Safe Deposit Boxes	concealing funds coming from illegal sources in safe deposit boxes	2	3	2.4
Economic activity (in general)	use of existing economic operators to launder money	2	4	2.8
	use of non-business companies for money laundering purposes	2	4	2.8
	use of intermediation of others entities to legitimise funds coming from illegal activities	3	4	3.4

1001. The estimate of the overall level of probability in the area of money laundering for the assessment of residual risk has been calculated at around 2.67, which is a high level. On the other hand, the risk of money laundering in the scope of residual risk is approx. 2.00 and it is at an average level.[500]

8.1.3. Assessment of general risk

1002. The assessment of general risk of money laundering is based on correlating the residual risk estimate with the underlying risk estimate using a formula: $R_O=33{,}3\%*R_P+66{,}7\%*R_S$[501]. On this basis, the estimate of the overall risk of money laundering amounts to approx. 1.95 and it is at an average level.

[500] Calculated according to the formula: $R_s=60\%*P_p+40\%*K_{rp}$; where: R_s - level of residual risk, P_p - level of probability of using elements of the Polish economy, K_{rp} - level of money laundering consequences to assess underlying risk.

[501]where: R_O - general risk level,R_P - underlying risk level, R_S - residual risk level.

8.2. RISK ASSESSMENT OF FINANCING OF TERRORISM

8.2.1. Assessment of underlying risk

Level of threat

1003. Poland is a country where the terrorist threat is at one of the lowest levels in Europe. However, it should be borne in mind that the geopolitical situation and our country's involvement in stabilisation activities in Afghanistan, Iraq and other international activities may trigger interest in Poland as a target for terrorist attacks. As a function of the terrorist threat, the threat of financing of terrorism on the territory of the Republic of Poland, similarly to the terrorist threat itself, is currently relatively low - despite the fact that Poland as a country may be considered as an attractive place for building logistics facilities and financial resources by terrorist organisations (due to, among others, a good location at the intersection of trade and communication routes, membership in the Schengen Area and the alleged lower counter-terrorist regime).

1004. According to the 2018 data obtained from the Ministry of Justice, Polish courts did not conduct criminal proceedings in connection with crime under Article 165a of *the Penal Code* in the analysed period. On the other hand, in 2017, in one case, court proceedings were initiated against three persons in connection with committing an offence under Article 165a of *the Penal Code* . These persons were sentenced in the first instance for the above mentioned offence, and in 2018 the sentences became final. In accordance with the indictment, the allegations concerning the financing of terrorism related to foreign means of payment in the total amount of EUR 8 950, intended in particular as the material support for members of armed groups operating within the structure of the terrorist organisation called the Caucasus Emirate and carrying out armed activities on the territory of the Russian Federation. As the judge conducting the case stressed in the justification of the verdict, the activity of the accused did not threaten the security of the Republic of Poland but it mainly affected the interests of another state - the Russian Federation. The above-mentioned amount is three times lower than the level of estimated assets subject to financing of terrorism on an annual basis corresponding to a low level of threat of financing of terrorism (EUR 8,950 < 0.000005%* of GDP).

1005. Poland is a member of the EU and a signatory to the Schengen Agreement - an agreement of 1985 abolishing checks at internal borders of signatory states. The resulting freedom of movement of persons within the so-called Schengen area relates not only to citizens of the signatory states but to all persons of any nationality and citizenship who cross the internal borders in the area covered by the Agreement. The document drawn up for the needs of the European Commission concerning the transnational risk assessment of money laundering and financing of terrorism, which has an impact on the internal market and is related to cross-border activities, assesses that the EU internal market remains vulnerable to the risks related to money laundering and financing of terrorism. Terrorists use a wide range of methods to raise and move funds, taking advantage of new opportunities arising from the emergence of new services and products. The product risk of financing of terrorism resulting from the transnational risk assessment of money laundering and financing of terrorism is assessed as low but its level dangerously approaches the average.

1006. As regards the prevention of terrorist events in the Polish counter-terrorist system, the Head of the ABW plays a leading role in identifying threats related to terrorism. He also coordinates analytical and information activities and the exchange of information between services as regards terrorist incidents and is responsible for coordinating the operational and exploratory activities of other services in this area. The cooperation between the services and institutions of the Polish counter-terrorist system consists primarily in providing any information obtained by the system members which is included in the catalogue of incidents and events to be reported to CAT ABW. E.g. While performing its statutory tasks related to counteracting financing of terrorism in 2017, the GIFI initiated 37 analytical proceedings (in 2018 - 41 analytical proceedings) related to transactions and activities which potentially could have been related to financing of terrorism. As a result of the analyses related to the above mentioned topics, in 2017, the GIFI submitted 45 notifications (in 2018 - 53 notifications) to the Internal Security Agency. The ABW verifies the signals received regarding possible transfers/transfers of funds - for the purpose of financing of terrorism - that are submitted to the Agency from partner services and institutions or are obtained in the course of operational work. The information thus acquired mostly relates to transfers performed through financial institutions or the Hawala system. However, due to the nature of the phenomenon, it is difficult to confirm the actual involvement of a person or entity in financing of terrorism.

1007. Pursuant to *the Act of 10 June 2016 on counter-terrorist activities* , the Prime Minister, after consultation with the Minister competent for internal affairs and the Head of the ABW, and in urgent situations - the Minister competent for internal affairs (who will inform the Prime Minister immediately), after consultation with the Head of the ABW, may introduce, by way of a regulation, alert levels depending on the type of threat of a terrorist event. Since 2016, five alert levels have been introduced in Poland[502]:

1) NATO 2016 Summit in Warsaw - the first ALFA alert level was introduced in the area of the capital city of Warsaw which was valid from 7 July to 10 July 2016.
2) 31st World Youth Day 2016 in Kraków - the first ALFA alert level and the second BRAVO CRP alert level were introduced across the country, which was valid from 20 July to 1 August 2016.
3) Session of the Conference of the Parties to the UN Framework Convention on Climate Change (COP24) in Katowice - the first ALFA alert level was introduced on the territory of the Silesian Province and the city of Kraków, which was valid from 26 November to 15 December 2018.
4) Ministerial meetings on security in the Middle East in Warsaw - the first ALFA alert level and the second BRAVO CRP alert level were introduced in the area of the capital city of Warsaw, which were valid from 11 February to 15 February 2019.
5) Elections to the European Parliament in 2019 - the second level of the BRAVO-CRP alert was introduced across the entire territory of the Republic of Poland, which was valid from 23 May 2019 until 27 May 2019.

1008. In comparison with the neighbouring countries of Poland, the level of financing of terrorism threat of our country is not high. The Russian national assessment of financing of terrorism risk evaluates the overall level of financing of terrorism threat as medium, while pointing out that the increased threat to financing of terrorism is influenced by Russia's

[502] The highest was the BRAVO-CRP level which is introduced when there is an increased and predictable threat of a terrorist incident but the specific target of the attack has not been identified.

participation in the long-lasting conflict in Syria and Iraq and by the perceived influence of ISIS, which acts as a catalyst for financing of terrorism in the Russian Federation.[503] In the Federal Republic of Germany, no terrorist alert system is effective. The Federal Ministry of the Interior (German: *Bundesministerium für Inneres*) does not communicate the degree of the terrorist attack risk to the public. However, according to this ministry, the terrorist threat in Germany remains high[504] The same level applies to financing of terrorism threat in this country, as a function of the terrorist threat. On the basis of the information held by this country, Slovakia assesses its level of terrorist threat and financing of terrorism threat as low[505] Lithuania[506] assesses its level of financing of terrorism threat in the same way, taking into account the fact that for several years there have been no identified cases of financing of terrorism involving foreign entities in the country. The Czech national assessment of money laundering and financing of terrorism risk states that the threat of financing of terrorism is an extremely serious crime, but currently no such cases are detected in the Czech Republic[507] On the other hand, the level of financing of terrorism threat in Ukraine, which results from the national assessment of the risk of money laundering and financing of terrorism of this country, is assessed as high[508] The high level of the threat of terrorism and financing of terrorism results from the country's armed conflict, the loss of the Crimea to the benefit of Russia as well as Russia's inspiring and supporting separatist and diversionary and terrorist activities of *quasi states* in the Donetsk and Lugansk regions of Ukraine. The Belarusian authorities, on the other hand, present the opinion that the country, due to the fact that it is only a transit country for suspicious funds and shows features of low risk from the point of view of financing of terrorism[509]

1009. Given the above, it must be concluded that the level of financing of terrorism threat is low (albeit tending to be close to average).

Level of vulnerability

1010. According to the methodology adopted, the level of vulnerability is the same as estimated for money laundering vulnerability in the area of underlying risk, i.e. at a medium level. The justification is presented in subchapter 8.1.1.

---

[503] The Russian Federation national terrorism financing risk assessment 2017-2018. Public Report, Federal Financial Monitoring Service, Moscow 2018, p. 22-23, available at: http://www.fedsfm.ru/en/preparation-fatf-fourth-round/national-terrorist-risk-assessment.

[504] https://wiadomosci.wp.pl/szef-msw-niemiec-w-kazdej-chwili-trzeba-sie-liczyc-z-zamachem-terrorystycznym-6301647794869889a, date of reading 27 June 2019

[505] National assessment of the risk of money laundering and terrorist financing, Slovakia, p. 204, available at: https://www.minv.sk/swift_data/source/policia/fsj/mv/ANNEX 34.pdf.

[506] Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing, Vilnius 2015, p. 21, available at: - http://www.fntt.lt/data/public/uploads/2016/10/d3_lnra2015.pdf.

[507] Report on the first round of national money laundering and terrorist financing risk assessment, Czech Republic, December 2016, p. 108, available at: http://www.financnianalytickyurad.cz/download/FileUploadComponent-1029799670/1524655342_cs_report-od-the-first-round-of-nat-ml_ft-risk-assessment.pdf.

[508] National risk assessment report on preventing and countering legalization (laundering) of proceeds of crime and financing of terrorism, Ukraine, Kiev 2016, p. 195, available at: http://www.sdfm.gov.ua/content/file/Site_docs/2017/20170113/nra.pdf.

[509]https://www.belarus.by/en/press-center/speeches-and-interviews/opinion-belarus-is-low-risk-country-for-terrorism-financing_i_0000089058.html , date of reading 27 June 2019

Level of consequence

1011. The available information does not indicate a significant level of terrorist activity in the country or in terms of financing terrorist activities. No increase in criminal activity from which funds designated for the terrorist activities could originate has been found.

1012. The other elements which have been indicated for estimating the level of consequences of financing of terrorism for the underlying risk assessment are the same as the basis for estimating the consequences of money laundering for the underlying risk assessment. They were taken under consideration and described in subchapter 8.1.1.

1013. In view of the foregoing, the consequences in the area of financing of terrorism in terms of the underlying risk can be estimated at a low level (i.e., describing them as weak consequences).

Underlying risk estimation

1014. In accordance with the methodology presented in Annex 1, the estimate of the underlying risk in the area of financing of terrorism should be calculated according to the formula: $R_{rp\_ft}=60\%*P_{rp\_ft}+40\%*K_{rp\_ft}$[510], where $P_{rp\_ft} = 40\%*Z_{rp\_ft}+60\%*P_{rp\_ft}$[511]. Based on the last formula, the probability level of financing of terrorism for the purpose of assessment of the underlying risk, i.e. P_{rp_ft} is 1.60, which is an average level. On the other hand, in accordance with the first formula, the financing of terrorism risk in the scope of underlying risk is 1.36 and it is at a low level.

8.2.2. Assessment of residual risk

Level of threat

1015. Annex no. 3 presents financing of terrorism risk scenarios, compiled on the basis of both domestic and foreign experience . For each of them, the level of vulnerability and threats were estimated, presented in Table no. 30 below.

Table No. 30 - Vulnerability, threat and probability levels for individual financing of terrorism risk scenarios

Area	Risk description	Level of vulnerability	Level of threat	Level of probability[512]
Banking	using the bank account to collect and transfer money for terrorist activities	2	4	2.8
	borrowing from financial institutions without an intention to repay the resulting liabilities	2	3	2.4
	use of anonymous prepaid cards in order to make it more difficult to	2	1	1.6

[510] where: R_{rp_ft} - level of "underlying risk", P_{rp_ft} - level of money laundering probability to assess the "underlying risk", K_{rp_ft} - level of money laundering consequences to assess the "underlying risk".

[511] where: Z_{rp_ft} - money laundering threat level to assess the "underlying risk", P_{rp_ft} - Money laundering vulnerability level to assess the "underlying risk".

[512] Calculated in accordance with the formula presented in Annex 1, i.e: $P_{ps\_ft}=40\%*Z_{ps\_ft}+60\%*P_{ps\_ft}$; where: P_{ps_ft} - probability level for the scenario, Z_{ps_ft} - threat level for the scenario, P_{ps_ft} - vulnerability level for the scenario.

	identify persons carrying out financing of terrorism transactions			
	use of transfers in order to transfer funds to other jurisdictions	2	3	2.4
Payment services (offered by entities other than banks)	the use of money transfer service providers to transfer assets designated for financing of terrorism	2	3	2.4
	use of online payment services by entities involved in the process of financing of terrorism, in particular by potential foreign terrorist militants	3	3	3
	Use of the *Hawala* network or other informal asset transfer systems for financing of terrorism	4	2	3.2
Insurance	fraud of compensations from insurance for the purpose of financing of terrorism	4	1	2.8
	allocating money from the policy for financing of terrorism	1	1	1
Other financial institutions	using a FOREX brokerage company for fraud to raise funds for terrorist activities	2	1	1.6
	trading in participation units in investment funds for the purpose of collecting funds for terrorist activities	2	1	1.6
	use of securities accounts and cash accounts to handle them in order to accumulate funds for terrorist activities	2	1	1.6
Currency exchange	currency exchange to make it more difficult to identify financing of terrorism offences	2	2	2
	exchange of low-denomination money to higher value banknotes	2	2	2
	cashless currency exchange combined with the transfer of funds	2	2	2
Virtual currencies	use of cryptocurrency for the transfer of property values for terrorist activities	3	2	2.6
Telecommunication services linked with mobile payments	purchasing or recharging SIM cards to transfer funds	4	1	2.8
	use of telecommunication services in the field of enhanced payment numbers to accumulate funds terrorist activity	4	2	3.2
Physical carriage of property values across borders	use of natural persons to transport money coming from illegal sources across state borders	4	3	3.6
	courier or postal service providers,	3	2	2.6
Gambling	funds obtained illegally to promote terrorism were laundered through online gambling	2	1	1.6

Non-profit organisations	use of funds raised for charitable purposes to finance terrorist organisations	3	2	2.6
Crowdfunding	raising funds for terrorist organisations through modern communication networks	4	2	3.2
Trading in high value goods	stones and precious metals robbed by terrorists are smuggled into other countries for sale	3	1	2.2
	purchase of stolen antiques and works of art from persons involved in terrorist activities	3	1	2.2
Economic activity (in general)	use of existing economic operators for financing of terrorism	2	2	2
	use of non-business companies for financing of terrorism	2	2	2
Social benefits	use of social benefits by foreign terrorist militants	3	1	2.2

1016. The estimate of the overall level of probability in the area of financing of terrorism for the assessment of residual risk has been calculated at around 2.33, which is a average level. On the other hand, the risk of financing of terrorism in the scope of residual risk is approx. 1.80 and it is at an average level.[513]

8.2.3. Assessment of general risk

1017. The assessment of general risk of financing of terrorism is based on correlating the residual risk estimate with the underlying risk estimate using a formula: $R_{O\_ft}=33,3\%*R_{P\_ft}+66,7\%*R_{S\_ft}$[514]. On this basis, the estimate of the overall risk of financing of terrorism amounts to approx. 1.65 and it is at an average level.

[513] Calculated according to the formula: $R_{s\_ft}=60\%*P_p+40\%*K_{rp\_ft}$; where: R_{s_ft} - level of residual risk, P_{p_ft} - level of probability of using elements of the Polish economy for terrorist financing, K_{rp}_ft - level of terrorist financing consequences to assess underlying risk.

[514]where: R_{O_ft} – general risk level, R_{P_ft} – underlying risk level, R_{S_ft} – residual risk level.

9. CONCLUSIONS OF THE NATIONAL ASSESSMENT OF THE RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM

1018. Estimates of the average level (i.e. level 2 on a four-level scale) of the risk of money laundering as well as financing of terrorism indicate that the national anti-money laundering and anti-terrorist financing system should be further improved in order to optimise its functioning. It is important both to improve the legal provisions which form its basis as well as the tools used within its framework, including procedures, ICT systems, and to develop training and exchange of information between entities involved in this system.

1019. Based on the information presented in subchapter 7.1, it is important for the effective functioning of the Polish anti-money laundering and counter-terrorist financing system to undertake or continue activities in the area of four issues related to legal regulations:

- completing the implementation of the provisions of Directive 2015/849;
- implementation of the provisions of Directive 2018/843;
- completing the works on 3 implementing regulations to *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* (for the issuance of which statutory delegations were indicated in Article 79(3), Article 84(4) and Article 84(4) of the aforementioned Act);
- completion of the legislative process related to the draft *Act amending the Act on Foreign Exchange Law and certain other acts* (relating to the regulation of issues related to the so-called online bureaux de change offices)[515].

1020. Complementary legislation also raises other issues relating to the practical implementation of the tasks of the entities involved in the national anti-money laundering and counter-terrorist financing system. First of all, it concerns issues related to the functioning of ICT systems. Currently, the GIFI ICT system is undergoing reconstruction which serves the purpose of receiving, processing (including the analysis) and making available the information referred to in *the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* . It is essential - for an efficient data analysis as well as for the seamless examination of the effectiveness not only of the GIFI activities but also of the entire national anti-money laundering and counter-terrorist financing system - that information is provided and processed electronically, in a structured form, allowing for quick analysis, including the generation of

[515] https://bip.kprm.gov.pl/kpr/form/r18139195608452,Projekt-ustawy-o-zmianie-ustawy-Prawo-dewizowe-oraz-niektorych-innych-ustaw.html, date of reading 28 June 2019

statistical data based on various criteria, needed both for management control and for conducting of *strategic analysis*[516].

1021. The issue of supplying the GIFI ICT system with input data appropriate in terms of type and form is associated with ensuring, on the one hand, adequate information from the obligated institutions and cooperating units in terms of quality and, on the other hand, sufficient knowledge to perform duties in this respect. In the first area - in addition to the completion of work on the drafts of three aforementioned executive regulations to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* and the implementation of their provisions - it is worth considering undertaking work on the preparation of an optional executive regulation, referred to in Article 109 of the above Act. In the second area (however, closely related to the first one) - it is important to provide appropriate training both for employees of the financial intelligence unit, cooperating units and obligated institutions and a platform for the exchange of knowledge and experience.

1022. In February 2019, the GIFI launched a new edition of the e-learning course entitled "Counteracting money laundering and financing of terrorism" addressed to employees of obligated institutions as well as cooperating units. However, periodic exchange of information at different levels is also needed. First of all, the cooperation of the GIFI and the cooperating units with obligated institutions is important in terms of exchanging knowledge and experience in the area of counteracting and combating money laundering and financing of terrorism (especially in terms of newly identified threats or vulnerabilities). The first step, which has already been taken in this direction, was the adoption by the FSC in May 2019 of *the resolution on the establishment of a Working Group for the cooperation of representatives of the public, private and public-private sectors.*

1023. Besides providing human resources appropriate for the implemented tasks, it is also crucial to develop the knowledge and skills of employees of the financial intelligence units and law enforcement agencies in the scope of conducting the so-called operational analysis[517] and financial investigation[518] through providing periodical training in this area. In addition, it is important to ensure training to employees of the judiciary in the scope of combating money laundering and financing of terrorism.

1024. In order to examine the effectiveness of the national system of money laundering and financing of terrorism, not only data processed in the GIFI ICT system are important but also the effective processing of information held by law enforcement agencies and judicial authorities, in particular relating to ongoing criminal proceedings (not only concerning offences under Articles 165a and 299 of the *Penal Code* but also underlying offences), enabling quick and effective generation of statistical data as well as their easy comparison (in the case of data from different sources and related to different phases of criminal proceedings).

---

[516] The term defined in: International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated in October 2018, p. 95, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[517]Ibidem, p. 95.

[518]Ibidem, p. 98.