Ministry of Finance

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

Warsaw, 2023

TABLE OF CONTENTS

TABLE OF CONTENTS

Abbreviations and acronyms:

ABW	Internal Security Agency
AIF	alternative investment fund
AML/CFT	anti-money laundering and counter-terrorism financing
AIC	alternative investment company
ATS	Alternative Trading System
OPS	payment service office
CAT	ABW Counter-Terrorist Centre
CBA	Central Anti-Corruption Bureau
CBŚP	Central Investigation Bureau of the Police
CPT ABW	ABW Terrorist Prevention Centre
CRBO	Central Register of Beneficial Owners
VPF	voluntary pension fund
GNI	gross national income
Journal of Laws	Journal of Laws of the Republic of Poland
OJ	Official Journal of the European Union
ECB	European Central Bank
ESMA	European Securities and Markets Authority
ESW	Egmont Secure Web, i.e. the IT system developed within the Egmont Group and used by FIUs 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 its 40 recommendations defining the international standards concerning counteracting money laundering as well as financing of terrorism and proliferation)
OEIF	open-end investment fund

FIU.net	system for the exchange of information between financial intelligence units of EU Member States
CEIF	closed-end investment fund
FTP	foreign terrorist fighters
GIFI	General Inspector of Financial Information
GPW S.A.	Giełda Papierów Wartościowych w Warszawie S.A. (Warsaw Stock Exchange)
GUS	Statistics Poland
IBnGR	Gdańsk Institute for Market Economics
ICO	initial coin offering
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 FATF Recommendation No. 29, the financial intelligence unit means "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 financing of terrorism, and for the dissemination of the results of the analysis", that "should be able to obtain additional information from obligated institutions and should have access to timely financial, administrative and criminal information that it requires to perform its functions properly")
KAS	National Revenue Administration (Polish: *Krajowa Administracja Skarbowa*)
KBF	Financial Security Committee (Polish: *Komitet Bezpieczeństwa Finansowego*)
KCIK	National Centre of Criminal Information (Polish: *Krajowe Centrum Informacji Kryminalnych*)
KDPW S.A.	Krajowy Depozyt Papierów Wartościowych S.A. (National Depository of Securities)

KGP	Police Headquarters
DPI	domestic payment institution
PC	Penal Code
PFC	Penal Fiscal Code
KNF	Polish Financial Supervision Authority (Polish: *Komisja Nadzoru Finansowego*)
KRS	National Court Register (Polish: *Krajowy Rejestr Sądowy*)
CCPC	Code of Commercial Partnerships and Companies
MONEYVAL	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 for the monitoring and assessment of the compliance of the MONEYVAL member states with key international AML/CFT rules, as well as of the 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 involving the acceptance of cash, cheques, other monetary instruments and values and the payment 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 referred to as Hawala, hundi and fei-chen)
NBP	National Bank of Poland
NPO	non-profit organisation
NSA	Supreme Administrative Court (Polish: *Naczelny Sąd Administracyjny*)
OECD	Organization for Economic Co-operation and Development
OPF	open pension fund
OIC	Organisation of Islamic Cooperation
OTF	organised trading facilities other than a regulated market or an ATS
GDP	Gross Domestic Product
EPFC	employee pension fund companies

RP	Republic of Poland
RWE	right-wing extremist
SAR	Suspicious Activity Report
SOIF	specialised open-end investment fund
BG	Border Guard (Polish: *Służba Graniczna*)
SKOK	cooperative savings and credit union
SKW	Military Counterintelligence Service
SWW	Military Intelligence Service
STIR	ICT system of the clearing house, referred to in the provisions of Section 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 2651)
STR	Suspicious Transaction Report
TFTP	Terrorist Finance Tracking Program
EU	European Union
UKE	Electronic Communications Authority (Polish: *Urząd Komunikacji Elektronicznej*)
UKNF	Office of the Polish Financial Supervision Authority (KNF)
VAT	value-added tax
WSA	Voivodeship Administrative Court (Polish: *Wojewódzki Sąd Administracyjny*)
MP	Military Police

1. INTRODUCTION

1. Over the last few years, there have been significant changes in both the threats of and vulnerabilities to money laundering and financing of terrorism in Europe and worldwide. We can hear increasingly often about using new financial solutions to commit the aforementioned offences. An increase in the level of risk in the above area results, among others, from the dynamic development of crypto-assets. It is worth noting that in its 2022 supranational assessment of the risk of money laundering and financing of terrorism, the European Commission assessed the crypto-asset-related money laundering and terrorism financing risk at the highest level on a 4-point scale. At the same time, legislative changes have been made in the European Union since 2021, in particular as part of the AML/CFT package, aimed at, among others, mitigating this risk[1].

2. The pandemic and the full-scale war initiated by Russia in Ukraine have caused some changes in the level of threats resulting from certain predicate offences or geographical directions. This issue has been raised, among others, by the FATF, that expressed serious concern in its public statements, especially about the impact of Russian aggression on increasing the risk of money laundering and financing of terrorism or proliferation, as Russia's actions violated the FATF core principles that aim to promote the security, safety and integrity of the financial system.

3. As a country located centrally in Europe and bordering the fighting Ukraine, Poland is also exposed to the risks resulting from the aforementioned phenomena. The latest *Act on counteracting money laundering and financing of terrorism* adopted in 2018 (Journal of Laws of 2023, item 1124) and its later amendments as well as the provisions of other related acts, such as the *Act on the Financial Information System*, provided the grounds for improving the structure and operation of the national system for counteracting money laundering and financing of terrorism. This does not mean, however, that we should consider these improvements sufficient and refrain from further ones. Therefore, the main purpose of this National Assessment of the risk of money laundering and financing of terrorism is to verify the aforementioned system in terms of what other areas thereof should be improved.

[1] *On 9 June 2023, REGULATION (EU) 2023/1113 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 was published in the Official Journal of the European Union.*

2. FINANCIAL MARKET AND NON-FINANCIAL MARKET IN POLAND

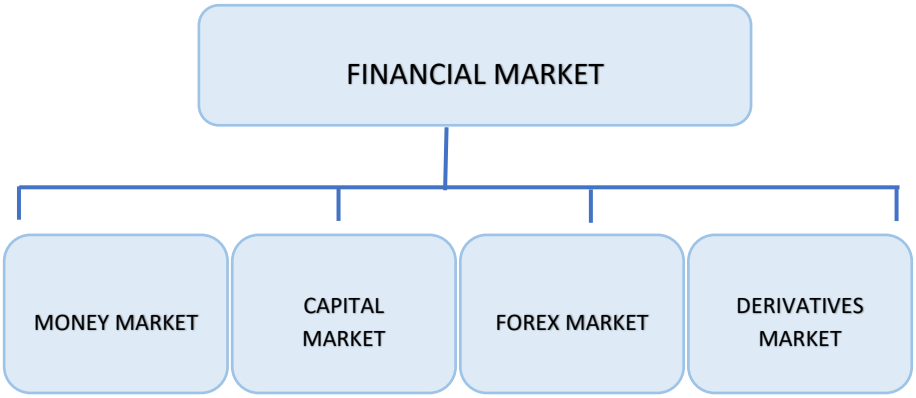
2.1. FINANCIAL MARKET IN POLAND

2.1.1. Introduction

4. The financial market in Poland has been developing since the early 1990s, with a significant increase in the number of concluded transactions and the overall scale of turnover. Financial market participants include, on the one hand, entities in need of capital, creating demand, and on the other hand, entities having free cash, creating capital supply.

5. The financial market consists of various segments, each of which plays a different role in satisfying the needs of financial market participants.

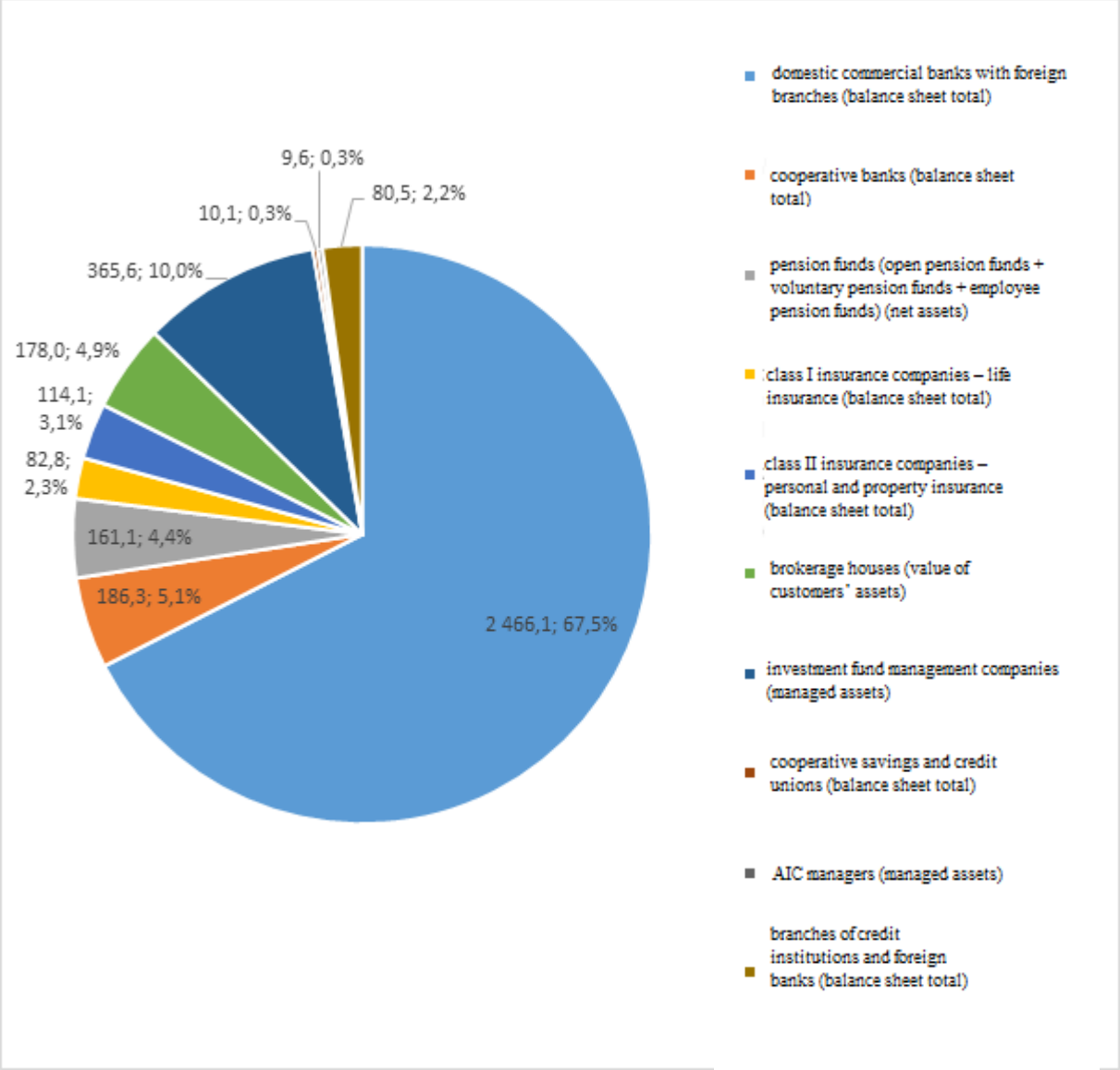
Diagram 1. Financial market breakdown



6. The financial market in Poland is supervised by the Polish Financial Supervision Authority (KNF), established under the *Act of 21 July 2006 on financial market supervision* (Journal of Laws of 2023, item 753). The supervision exercised by this institution covers, among others, the banking sector, capital market, insurance market, pension market, payment institutions and payment service offices, electronic money institutions, and the cooperative savings and credit union sector.

7. The banking sector was the largest financial market segment out of all financial market segments supervised by the KNF in 2022. The greatest shares in the assets of the Polish financial sector were attributable to domestic commercial banks with foreign branches (67.5%), followed by investment fund management companies (10.1%) and cooperative banks (5.1%).

Chart 1. Structure of the Polish financial sector assets as at the end of December 2022 (in PLN billion)[2]



8. Supervision over the financial market is to ensure the proper operation of this market, its stability, security and transparency, trust in the financial market, and to protect the interests of its participants.

Table 1. Number of entities operating on the Polish financial market under the KNF supervision as at 31 December 2022[3]

Type of entity	Number of entities
Commercial banks (including 2 associating banks)	29

[2] Based on: *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2022 roku* (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2022), Warsaw 20.06.2023, p. 24 at: https://www.knf.gov.pl/?articleId=82835&p_id=18

[3] Ibidem, pp. 24-26.

State bank	1
Cooperative banks	496
Representative offices of foreign banks and credit institutions	9
Institutional Protection Systems (IPS)	2
Cooperative savings and credit unions, the National Association of Cooperative Savings and Credit Unions	20
Domestic payment institutions	42
Electronic money institutions	1
Entities providing only the account information access service	15
Small payment institutions	150
Payment service offices	1193
Mortgage brokers	804
Agents of mortgage brokers	7033
Brokerage houses	33
Banks conducting brokerage activities	9
Investment company agents	264
Custodian banks	11
Capital market infrastructure entities (Giełda Papierów Wartościowych w Warszawie S.A., Krajowy Depozyt Papierów Wartościowych S.A., KDPW CCP S.A., BondSpot S.A.)[4]	4
Issuers whose financial instruments have been admitted to trading on a regulated market[5], including: - issuers of shares for which Poland is the home country - issuers of bonds and covered bonds - foreign issuers	465
Issuers whose securities are introduced to an alternative trading system[6]	456
Investment funds	672
Investment fund management companies	55
AIC managers	324
Other entities providing services to investment funds or alternative investment funds, including entities entrusted with the performance of the duties of an investment fund management company or an AIC manager within the meaning of the Act on investment funds[7]	239
Commodity market infrastructure entities (Towarowa Giełda Energii S.A., Izba Rozliczeniowa Giełd Towarowych S.A.)	2
Commodity brokerage houses	1
Entities authorised to maintain exchange commodity accounts or registers	59
Open pension funds	10
General pension societies	9
Employee pension funds	2
Employee pension societies	2
Pension fund depositaries	5
Pension fund transfer agents	6
Voluntary pension funds	7

[4] Entities listed in Article 5 of the Act on capital market supervision, namely: companies operating a regulated market, Krajowy Depozyt Papierów Wartościowych S.A., companies operating a clearing house, companies operating a settlement house, the company to which Krajowy Depozyt Papierów Wartościowych S.A. delegated the performance of activities related to the tasks referred to in Article 48(1)(1)-(6) or Article 48(2) of the Act on trading, the central depository for securities within the meaning of Article (2)(1)(1) of Regulation 909/2014.

[5] Excluding closed-end investment funds whose investment certificates are admitted to trading on a regulated market.

[6] Direct supervision over the disclosure obligations of these issuers is exercised by companies operating a regulated market that organise an alternative trading system.

[7] The given number includes the number of distributors of participation units, transfer agents, fund depositories, external valuation entities, and entities authorised to manage securitised receivables of the securitisation fund.

Voluntary fixed-date pension funds	18
Class I insurance companies (life insurance)	24
Class II insurance companies /personal and property insurance/ and a reinsurance company (including two insurance companies in liquidation: - D.A.S. Towarzystwo Ubezpieczeń Ochrony Środowiska S.A. in liquidation (the KNF did not revoke the company's authorisation to conduct insurance business) and Towarzystwo Ubezpieczeń Wzajemnych MEDICUM in liquidation (the KNF revoked the company's authorisation to conduct insurance business)	318
Insurance brokers, including: - natural persons - legal persons Reinsurance brokers, including: - natural persons - legal persons	1,433, of which: 876 557 58, of which: 15 43
Insurance agents	29,092
Natural persons conducting agency business (Polish: OFWCA)	263,015

9. Entities conducting currency exchange activities are supervised by the President of the National Bank of Poland (NBP), as the body maintaining the register of currency exchange office operators, in accordance with the provisions of the *Act of 27 July 2002 – Foreign Exchange Law (Journal of Laws of 2022, item 309*).

10. Since 2020, the operation of the financial market in Poland has been largely affected by the global COVID-19 pandemic. This pandemic has contributed to a deep economic recession, which is primarily due to the large-scale restrictions (lockdown) introduced to minimise the spread of the SARS-CoV-2 virus.

11. The pandemic has caused significant changes in the classic model of banks' operation. The number of active users choosing banking services provided through electronic access channels has significantly increased, so has the number of cashless (contactless) transactions and electronic payments.

12. In 2021, as a result of the post-pandemic effect, there was a sharp increase in the prices of consumer goods, which triggered increased inflation and an increase in interest rates. Inflation in Poland reached levels not seen for decades. In September 2021, inflation in Poland was 5.9%[8]. At the end of December 2022, according to Statistics Poland, inflation reached 16.6%[9], to increase to 18.4% in February 2023. From March, it gradually decreased to reach 10.1% in August 2023.

13. In order to reduce inflation, the NBP interest rates were increased. In October 2021, interest rates increased from 0.1% to 0.5%, to further increase to 6.75% in September 2022.[10]

2.1.2. Financial market sectors

Banking sector

14. The banking sector is the largest part of the financial system in Poland, in terms of assets, financial results, created jobs and the number of customers. Poland ranks sixth in Europe in

[8] Raport o inflacji – Listopad 2021 (Report on inflation – November 2021), NBP, Warsaw, 2021, p. 6, at: https://nbp.pl/polityka-pieniezna/dokumenty-rpp/raporty-o-inflacji/

[9] GUS, https://stat.gov.pl/wykres/1.html

[10] Reference rate as at 8 September 2022, at: https://nbp.pl/polityka-pieniezna/decyzje-rpp/podstawowe-stopy-procentowe-nbp/, read on: 30.08.2023

terms of the number of individuals with access to banking services and employment in the banking sector, and second in terms of the number of banks.

15. The operation of banks in Poland is regulated by laws, including: *Act of 29 August 1997 – Banking Law* (Journal of Laws of 2022, item 2324), *Act of 29 August 1997 on the National Bank of Poland* (Journal of Laws of 2022, item 2025), *Act of 29 August 1997 on covered bonds and mortgage banks* (Journal of Laws of 2023, item 110), *Act of 10 June 2016 on the Bank Guarantee Fund, the deposit guarantee system and resolution* (Journal of Laws of 2022, item 2253), *Act of 19 August 2011 on payment services* (Journal of Laws of 2022, item 2360 – with respect to the operation of banks as payment service providers) and *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms*.

16. According to the Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2022, as at the end of 2022, the Polish Financial Supervision Authority (KNF) supervised 29 commercial banks (including two associating banks), 1 state bank, 2 institutional protection systems, 496 cooperative banks and 34 branches of credit institutions and foreign banks. In 2022, the Polish Financial Supervision Authority granted consent to carry out merger processes in the case of 10 cooperative banks. Moreover, in 2022, the Polish Financial Supervision Authority issued a decision authorising the Bank Guarantee Fund to establish, as the founder, a bridge institution under the name of Bank BFG Spółka Akcyjna. Bank BFG S.A. then changed its name to VeloBank Spółka Akcyjna.

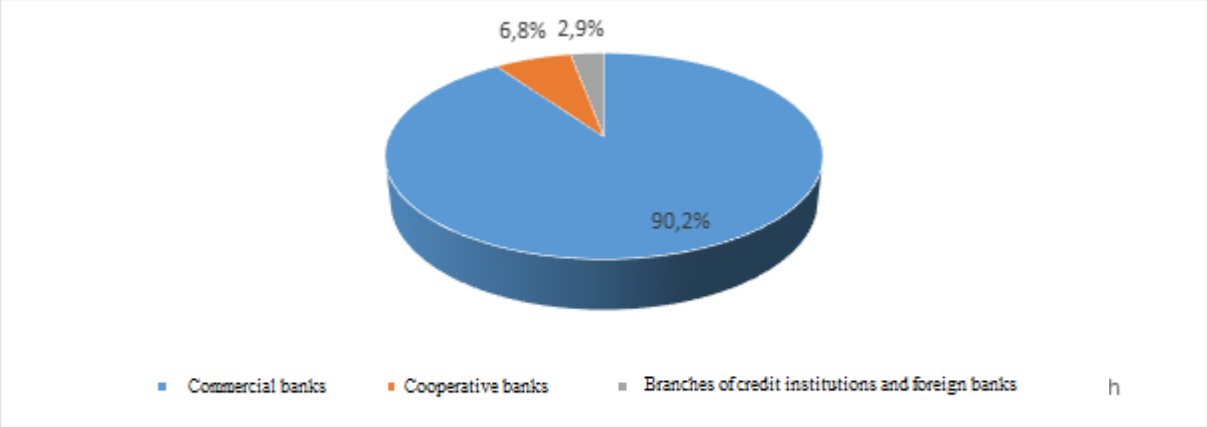
17. The average annual inflation in 2022 was 14.4% compared to 5.1% in 2021. The increase in prices was partially due to external factors, such as the increase in energy prices on global markets, supply chains that had not been yet reconstructed, and prolonged restrictions in China related to the "zero COVID" policy, limiting local production. The internal factors that contributed to the increase in inflation included expansionary fiscal policy, including aid programmes introduced in the wake of the COVID-19 pandemic, and expansive monetary policy. In the face of inflationary pressure in 2022, the Monetary Policy Council continued the series of interest rate hikes started in the second half of 2021. As a result, the reference rate in 2022 was increased by a total of 450 basis points (bps), from 2.25% to 6.75% at the end of 2022.

18. The profit of the banking sector as at the end of 2022 was PLN 12.1 billion (in 2021, the banking sector recorded a profit of PLN 6.0 billion). As at the end of 2022, assets of 19 cooperative savings and credit unions amounted to PLN 10 billion, and the total net profit of these entities was PLN 99.6 million.

19. As at the end of December 2022, the balance sheet total of the banking sector was PLN 2,732.9 billion and was 6.2% higher than in 2021. In terms of the balance sheet total, 90.2% of the banking sector is attributable to commercial banks with foreign branches – as at the end of 2022, their balance sheet total amounted to PLN 2,466.1 billion; in the case of cooperative banks, this figure was PLN 186.3 billion. The balance sheet total of branches of credit institutions and foreign banks amounted to PLN 80.5 billion.

Chart 2. Asset structure of the banking sector in 2022 by share of particular entities in the total value

of its assets[11]



20. In 2020-2022, there was a reduction in the number of bank branches (the bank network in Poland and abroad) and in the employment (in 2020-2021), caused largely by the COVID-19 pandemic that started in 2020. As at the end of 2022, the number of bank branches in Poland and abroad was 5,083, compared to 5,211 (in 2021) and 5,551 (in 2020). As regards employment reduction, a significant decrease in the number of bank employees was recorded between 2020 (149,003) and 2021 (143,049) (employment reduction by 5,954 individuals). As at the end of 2022, there was a slight increase in the number of employees in the banking sector (143,222 employees, i.e. an increase by 173 individuals).

Table 2. Number of banking sector entities[12] *in 2020-2022*

Number of banking sector entities	As at December 2020	As at December 2021	As at December 2022	Change
Commercial banks	30	30	30	0
Branches of credit institutions and foreign banks	36	37	34	-3
Cooperative banks	530	511	496	-15
Total	**596**	**578**	**560**	**-18**

Investment funds

21. The rules for the establishment and operation of investment funds registered in the territory of the Republic of Poland are provided for in the *Act of 27 May 2004 on investment funds and the management of alternative investment funds* (Journal of Laws of 2023, item 681).

22. An investment fund is a legal person whose sole activity consists in investing cash raised through public, and in the cases specified in the aforementioned act – also private, offering of the purchase of investment units or investment certificates in securities, money market

[11] Based on: Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2022 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2022), Warsaw 20.06.2023, at: https://www.knf.gov.pl/?articleId=82835&p_id=18

[12] Monthly data of the banking sector in Poland, at: https://www.knf.gov.pl/?articleId=56224&p_id=18

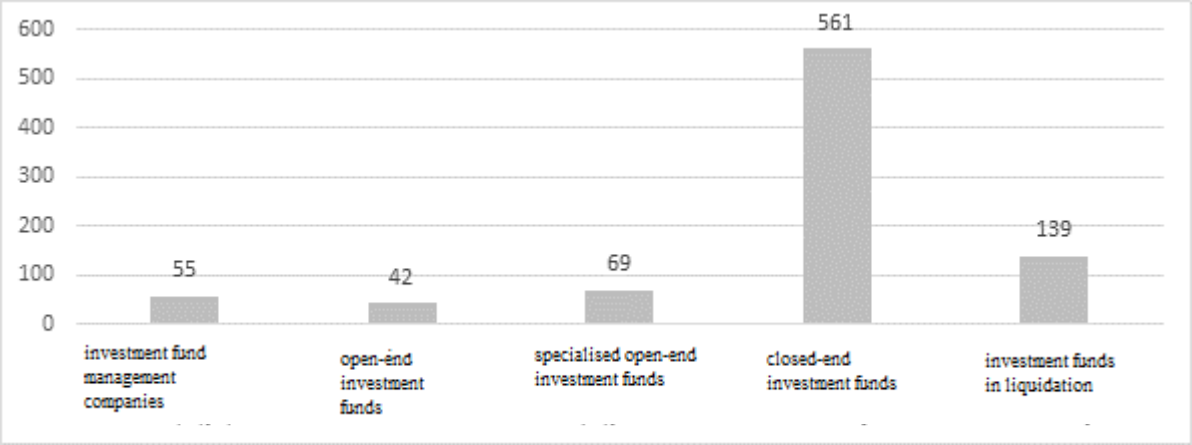
instruments, and other property rights specified in this act. An investment fund is managed by an investment fund management company.

23. The investment fund sector consists primarily of investment fund management companies managing open-end investment funds (FIO), specialised open-end investment funds (SFIO) and closed-end investment funds (FIZ).

24. The only investment funds operating in Poland and meeting the requirements of the *UCITS directive*[13] (i.e. funds harmonised with Community law) are open-end investment funds. Other investment funds, i.e. closed-end investment funds and specialised open-end investment funds, although the rules for their operation are regulated by the *Act on investment funds and the management of alternative investment funds*, do not meet the requirements of the *UCITS directive*. Pursuant to Article 3(4) of the aforementioned act, these funds are considered alternative investment funds (AIF).

25. As at 31 December 2022, there were 55 investment fund management companies authorised by the Polish Financial Supervision Authority, managing a total of 672 investment funds, including: 42 open-end investment funds, 69 specialised open-end investment funds, and 561 closed-end investment funds.

Chart 3. Number of investment fund management companies and investment funds in 2022[14]



26. As at 31 December 2021, the total value of net assets of investment funds amounted to PLN 322 billion (an increase of 7%, i.e. PLN 21 billion, compared to 2020). As at the end of 2021, not only did the total net assets of investment funds exceeded the level recorded before the COVID-19 pandemic, but it also reached the highest level in the last 5 years[15]. As at the end of 2022, the total value of net assets of investment funds amounted to PLN 284 billion, and

[13] 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 (OJ L 302, 17.11.2009, p. 32).

[14] Based on the data included in Raport dotyczący sytuacji finansowej towarzystw funduszy inwestycyjnych w 2022 r. (Report on the financial situation of investment fund management companies in 2022), UKNF, Warsaw, 2023, at: https://www.knf.gov.pl/?articleId=82429&p_id=18

[15] Raport dotyczący sytuacji finansowej towarzystw funduszy inwestycyjnych w 2021 r. (Report on the financial situation of investment fund management companies in 2021), UKNF, Warsaw, 2022, p. 5, https://www.knf.gov.pl/?articleId=78398&p_id=18

compared to the end of the previous year, it was lower by PLN 38 billion (i.e. 12%)[16]. The lower total profit of investment fund management companies was due to the revenue decline rate that was higher than that of cost reduction in 2022.

27. In 2021, investment fund management companies generated total revenue of PLN 3,635 million (an increase of 5.5% compared to 2020). The total costs incurred by investment fund management companies in 2021 amounted to PLN 2,636 million (an increase of 10.3% compared to 2020). The aggregated net financial profit of investment fund management companies amounted to PLN 763 million (a decrease of 9.9% compared to 2020)[17]. In 2022, revenue of investment fund management companies amounted to PLN 3.0 billion and was 17% lower than in 2021. Following the 2021 increase in total revenue, its value decreased to a level lower than that recorded in 2020. The 2022 decrease in total revenue was mainly due to a decrease in the level of its main component, i.e. revenue from investment fund management.

Pension funds

28. The rules for the establishment and operation of pension funds are laid down in the *Act of 28 August 1997 on the organisation and operation of pension funds* (Journal of Laws of 2023, item 930).

29. There are numerous institutions offering pension products in Poland, including entities offering various types of these products and entities specialising only in selected forms of these products.

30. In the second half of 2019, Employee Capital Plans (Polish: *Pracownicze Plany Kapitałowe* – PPK) were launched, and the obligation to implement them by employing establishments was made dependent on the number of employees and split into four stages. In 2020, despite the ongoing COVID-19 pandemic, the PPK implementation process continued, to include in its last stage (from 1 January 2021) public finance sector entities and other entities that had not been previously covered by this system. The introduction of PPKs significantly increased the popularity of another form of pension product, namely Employee Pension Schemes (Polish: *Pracownicze Programy Emerytalne* – PPE), numbering 2,083 as at the end of 2021 and 2,081 as at the end of 2022.

31. According to information received from institutions operating PPKs, as at the end of 2021, the number of individuals covered by PPKs was 2 million (compared to 1.5 million as at the end of 2020). During this period, PLN 4 billion was paid into PPKs (compared to PLN 2.2 billion in 2021). As at 31 December 2021, the balance of PPK accounts was PLN 6.2 billion (PLN 3.4 billion more than in 2020)[18]. As at the end of 2022, the number of PPK participants

[16] Raport dotyczący sytuacji finansowej towarzystw funduszy inwestycyjnych w 2022 r. (Report on the financial situation of investment fund management companies in 2022), UKNF, Warsaw, 2023, p. 5, at: https://www.knf.gov.pl/?articleId=78398&p_id=18

[17] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2021), Warsaw 2022, p. 75, at: https://www.knf.gov.pl/?articleId=78355&p_id=18

[18] Ibidem, p. 82.

was 3.0 million. During this period, PLN 5.3 billion was paid into PPKs. The balance of PPK accounts was PLN 12 billion[19].

32. As at the end of December 2021, there were 10 open pension funds and 10 general pension societies operating in Poland. Open pension funds had nearly 15.4 million members and their assets were worth PLN 187.9 billion[20]. As at 31 December 2022, open pension funds had 14.9 million members. Throughout the year, the number of their members declined by 0.3 million. The total market share of the three largest funds decreased slightly (by 0.1 p.p.) compared to the previous year, reaching almost half of the entire market (49.6%)[21].

33. In 2022, there was a decrease in the value of assets of pension funds managed by general pension societies (mainly as a result of a decrease in open pension funds' assets), at the same time, general pension societies received revenue from the refund of the overpayment from the Guarantee Fund, thus generating a higher profit than in the previous year.

34. As at the end of June 2021, two employee pension funds were operating in Poland. As at the end of June 2021, the number of employee pension funds' participants was 30,858 and their assets amounted to over PLN 2 billion[22]. As at 31 December 2022, employee pension societies managed two employee pension funds with their 29.4 thousand participants, i.e. fewer than a year earlier. In the period covered by the report, basic and additional premiums in the amount of PLN 107.3 million were transferred to the accounts of employee pension funds' participants, i.e. PLN 3.1 million more than in 2021. Both employee pension funds operating at the end of 2022 recorded negative rates of return in the reporting period[23].

Brokerage activities

35. The operation of brokerage houses and offices in the territory of Poland is regulated by the *Act of 29 July 2005 on trading in financial instruments* (Journal of Laws of 2023, item 646), while that of a commodity brokerage house is regulated by the *Act of 26 October 2000 on commodity exchanges* (Journal of Laws of 2023, item 652).

Table 3. Numbers of entities conducting brokerage and custody activities in 2018-2022[24]

Type of entity	2018	2019	2020	2021	2022

[19] Based on: Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2022 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2022), Warsaw, 20.06.2023, p. 56, at: https://www.knf.gov.pl/?articleId=82835&p_id=18

[20] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2021), Warsaw, 2022, pp. 76-77, at: https://www.knf.gov.pl/?articleId=78355&p_id=18.

[21] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2022 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2022), Warsaw, 20.06.2023, p. 54, at: https://www.knf.gov.pl/?articleId=82835&p_id=18

[22] https://www.gov.pl/web/finanse/fundusze-emerytalne-rynek-finansowy-i-dlugoterminowe-produkty-oszczednosciowe, access on 29.04.2022

[23] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2022 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2020), Warsaw, 20.06.2023, p. 54, at: https://www.knf.gov.pl/?articleId=82835&p_id=18

[24] Ibidem, p. 51.

Brokerage houses	*40*	*38*	*37*	*36*	*33*
Commodity brokerage houses	*1*	*1*	*1*	*1*	*1*
Banks conducting brokerage activities	*9*	*9*	*9*	*9*	*9*
Custodian banks	*12*	*12*	*11*	*11*	*11*
Total	**62**	**60**	**58**	**57**	**54**

36. As at 31 December 2022, brokerage houses (33 entities) maintained 920,793 financial instrument accounts[25], which represented a 17% increase compared to the previous year. It should be noted that over the last three years (2020 - 2022), the number of customer accounts maintained both in brokerage offices and brokerage houses was increasing[26]. As at the end of 2022, compared to the previous year, the value of total assets decreased by 14.3%, while the value of equity of the brokerage house sector increased by 24.5%. The decrease in the value of total assets was due to a decrease in customers' cash shown in the balance sheet of brokerage houses in 2022. As at the end of December 2021, brokerage houses maintained 789,481 financial instrument accounts, which represented a 27% increase compared to the previous year (2020), when this figure was 621,700. This business was conducted by 18 brokerage houses.

37. In 2022, the brokerage house sector recorded an increase in its net profit of PLN 927,126 thousand, i.e. 140% more compared to the previous year. The increased aggregate net profit of this sector was primarily due to higher profits generated by entities operating on the Forex market. According to the data contained in their December monthly reports, as at the end of 2021, brokerage houses generated net profit of PLN 386,041 thousand – a decrease compared to 2020 (PLN 584,424.1 thousand). The decline in the net profit of the brokerage house sector in 2021 was largely due to the decline in profits from operations involving financial instruments held for trading and the increase in the loss on its primary activity[27].

38. In 2021-2022, one commodity brokerage house was authorised to conduct brokerage activities involving the purchase or sale of exchange commodities on someone else's account, including the settlement of transactions and maintaining accounts or registers of exchange commodities.

39. According to its latest audited financial statements (for 2021), the only commodity brokerage house licenced by the Polish Financial Supervision Authority incurred in 2021 a loss in the amount of PLN 1,025,468.38, its equity amounted to PLN 6,479,589.76, and the amount of its total assets was PLN 8,095,698.44. According to the data contained in its December monthly report, in 2022, the commodity brokerage house generated a net profit of PLN 242,807,381.53 and its equity, as at 31 December 2022, amounted to PLN 249,286,971.29[28].

40. Commercial companies referred to in Article 50a of the *Act of 26 October 2000 on commodity exchanges*, i.e. commercial companies that are not commodity brokerage houses

[25] Customer accounts should be understood as both securities accounts and other financial instrument accounts.
[26] Raport o sytuacji finansowej domów maklerskich w 2022 roku (Report on the financial situation of brokerage houses in 2022), p. 5, at: https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_dot_sytuacji_finansowej_domow_maklerskich_w_2022_roku_82888.pdf
[27] Ibidem, p. 8
[28] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2022 roku (Report of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2022), pp. 25-26, at: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej

may conduct brokerage activities consisting in purchasing or selling exchange commodities on someone else's account, including the settlement of their principals' transactions and consultancy in the area of trading in exchange commodities.

41. As at 31 December 2021, custodian banks operated 39,670 securities accounts (a decrease of 1.46% compared to 31 December 2021) with assets worth PLN 816,453,065,550.00 (a decrease of 5.39% compared to 31 December 2021).

Insurers

42. Activities in the area of personal and property insurance business, reinsurance business, as well as the rules for performing the actuary profession, exercising insurance supervision, exercising supervision over insurance and reinsurance companies in groups, and the organisation and operation of insurance economic self-government are regulated by the *Act of 11 September 2015 on insurance and reinsurance business* (Journal of Laws of 2023, item 656).

43. As at the end of 2022, in class I (life insurance), 24 insurance companies were authorised to conduct insurance business (one fewer than in 2021). The balance sheet total of the insurance sector decreased throughout the year by 2.4% and as at the end of 2022, it was PLN 196.9 billion, of which PLN 82.8 billion was attributable to the companies in class I – life insurance, and PLN 114.1 billion to companies in class II – other personal and property insurance. In the period concerned, insurers generated a profit of PLN 6.1 billion (of which PLN 2.2 billion was attributable to class I and PLN 3.9 billion to class II)[29].

44. As at the end of Q4 2022, the structure of direct insurance in class I was dominated by life insurance (group 1), accounting for 45.16% of the gross premium written. Supplemental accident and sickness insurance (group 5), accounting for 34.91% of the gross premium written, came second, followed by group 3 insurance (life insurance, if related to an insurance capital fund, as well as life insurance in which compensation from the insurance company is determined based on specific indices or other base values), accounting for 18.80% the total premium of the class. In the four quarters of 2022, life insurance companies paid out claims and benefits in the amount of PLN 18.87 billion[30]. As at the end of 2021, the structure of direct insurance in class I was dominated by life insurance (group 1), accounting for 40.98% of the gross premium written. Supplemental accident and sickness insurance (group 5), accounting for 32.05% of the gross premium written, came second, followed by group 3 insurance (life insurance, if related to an insurance capital fund, as well as life insurance where compensation from the insurance company is determined based on specific indices or other base values), accounting for 25.76% the total premium of the class. The net profit of class I insurance companies was approx. PLN 1.63 billion, while income tax shown by the aforementioned insurance companies was approx. PLN 0.41 billion[31].

[29] Ibidem, pp. 22-23.
[30] Ibidem, p. 23.
[31] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2021 roku (Report of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2021), p. 21, at: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej

Payment institutions and electronic money institutions

45. The operation of payment institutions and electronic money institutions is defined in the *Act of 19 August 2011 on payment services*[32]. The payment services sector includes domestic payment institutions (DPI), small payment institutions (SPI) and payment service offices (PSO).

46. As at 31 December 2022, relevant registers included 42 domestic payment institutions, 150 small payment institutions, 15 providers rendering only the account information access service, 1 domestic electronic money institution, and 1,193 payment service offices. As at the end of Q4 2022, DPIs recorded own funds in the amount of PLN 1.05 billion. According to the DPI reporting information for the period from Q1 to Q4 2022 (as at 28 February 2023), DPIs performed in 2022 a total of 3.33 billion payment transactions worth PLN 470.72 billion, while SPIs performed in the same period 15.98 million transactions worth PLN 4.92 billion (as at 28 February 2023)[33]. As at 31 December 2021, relevant registers included 40 domestic payment institutions, 117 small payment institutions, 11 providers rendering only the account information access service, 1 domestic electronic money institution, and 1,262 payments service offices. As at the end of 2021, the own funds of domestic payment institutions amounted to PLN 677 million. According to the reporting information submitted to the KNF, during the four quarters of 2021, DPIs executed approx. 2.72 billion payment transactions in the total amount of approx. PLN 335.81 billion. In the same period, SPIs executed approx. 12.61 million transactions totalling approx. PLN 1.74 billion. To compare, Krajowa Izba Rozliczeniowa S.A. (Polish National Clearing House) processed in Elixir approx. 2.12 billion payment orders totalling approx. PLN 6.8 trillion. In the case of the number of transactions executed within the domestic payment institution sector, their total number was greater than the number of transactions executed in Eliksir – the foregoing applies to the number of low-value transactions[34].

Companies operating the regulated market

47. Companies operate the regulated market under the *Act of 29 July 2005 on trading in financial instruments*.

---

[32] This Act implemented 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 largely 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 in the Journal of Laws, that implemented into the Polish legal system 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 and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p.35).

[33] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2022 roku (Report of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2022), p. 22, Warsaw 2023

[34] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2021 roku (Report of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2021), p.21, Warsaw, 2022

48. The operation of the regulated market is supported by capital market infrastructure entities, including GPW S.A., BondSpot S.A., Towarowa Giełda Energii S.A., Izba Rozliczeniowa Giełd Towarowych S.A. and Krajowy Depozyt Papierów Wartościowych S.A. (KDPW S.A.) and KDPW_CCP S.A.

49. Besides the regulated market, GPW S.A. also operates an organised market of financial instruments in the form of an alternative trading system, i.e. NewConnect and ASO Catalyst. It is intended primarily for young companies with relatively small expected capitalisation. Financial instruments traded on NewConnect include mainly shares and rights to shares of small and medium-sized companies, while those traded on ASO Catalyst include debt instruments.

50. In 2022, only one public offering was carried out on the GPW main market, the remaining 15 ones were carried out on NewConnect. Some offerings were suspended or cancelled and were not carried out in 2022, which was primarily due to market sentiment determined by the war in Ukraine and high uncertainty in markets around the world[35]. In 2021, share trading on the GPW market increased compared to the previous year, with a simultaneous decrease in share trading on NewConnect[36].

51. Trading on the regulated market is also conducted by BondSpot S.A., supervised by the Polish Financial Supervision Authority. It mainly deals with trading in treasury, corporate and cooperative bonds, as well as other debt securities. BondSpot S.A. also organises trading in debt instruments within the alternative trading system (these instruments may include dematerialised bonds, covered bonds and other debt financial instruments incorporating property rights corresponding to the rights arising from incurring a debt). It also operates a second alternative trading system, called Treasury BondSpot Poland (TBSP), with the highest turnover value, which has decreased significantly in recent years. However, in 2021, a higher turnover value was recorded than in 2018 (PLN 407 billion), amounting to PLN 474 billion[37]. On 28 June 2022, the Annual General Meeting of BondSpot adopted a resolution on the distribution of the 2021 profit of BondSpot, allocating, among others, PLN 1,000 thousand for the payment of dividend. The dividend payable to GPW amounted to PLN 972 thousand. The dividend was paid on 28 July 2022[38].

52. In 2021, for the first time since 2017, there was an increase in the number of issuers whose shares were listed on the GPW regulated market (i.e. 430 entities) or in the NewConnect alternative trading system (i.e. 380 entities). As at the end of 2021, there were 430 GPW-listed companies, including 383 domestic and 47 foreign ones. In the reporting period, there were 16 IPOs (including three of foreign companies) and 19 withdrawals (including five of foreign

[35] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2022 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2022), Warsaw, 20.06.2023, p. 57, at: https://www.knf.gov.pl/?articleId=82835&p_id=18

[36] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2021), Warsaw, 2022, pp. 82-83.

[37] Ibidem, p. 84.

[38] Jednostkowe sprawozdanie finansowe Giełdy Papierów Wartościowych w Warszawie S.A. za rok zakończony 31 grudnia 2022 r. (Separate financial statements of Giełda Papierów Wartościowych w Warszawie S.A. for the financial year ended on 31 December 2022), p. 65, at: https://www.gpw.pl/pl-ri-raporty-okresowe

companies) – as a result, the number of listed companies did not increase for the sixth year in a row[39].

53. The COVID-19 pandemic that started in March 2020 had a significant impact on the operation of GPW S.A. The resulting restrictions on running business, aid programmes and tax reliefs, and, above all, increased uncertainty on financial markets had a significant impact on the volatility of capital markets, which translated into the value of turnover and capitalisation of companies on the Main Market of GPW S.A. As a result, in 2020, there was a significant increase in GPW S.A. revenue and improvement in its financial results, maintained also in 2021. In 2022, revenue of PLN 389.3 million was recorded (i.e. 4.5% lower than in 2021).

54. As at 31 December 2022, GPW had PLN 154 million of cash and cash equivalents as well as short-term financial assets in the form of bank deposits and guaranteed corporate bonds (compared to PLN 466 million in 2021). These financial resources are sufficient to conclude that the risk of loss of liquidity by the Company in the short and medium term is low[40].

Cooperative savings and credit unions[41]

55. The operation of cooperative savings and credit unions (Polish: *Spółdzielcza Kasa Oszczędnościowo-Kredytowa* – SKOK) is regulated by the *Act of 5 November 2009 on cooperative savings and credit unions* (Journal of Laws of 2023, item 1278), and to the extent not regulated in the aforementioned act – the provisions of the *Act of 16 September 1982 – Cooperative Law* (Journal of Laws of 2021, item 648).

56. As at the end of Q4 2022, there were 19 SKOKs and the National Association of Cooperative Savings and Credit Unions (20 entities in total). In 2022, three SKOKs merged with other SKOKs with the consent of the Polish Financial Supervision Authority.

57. As at 31 December 2022, SKOKs showed a total profit of PLN 99.59 million (as at the end of December 2021, 22 SKOKs operating at that time showed a profit of PLN 7.43 million).

58. Compared to the end of 2021, own funds of the SKOKs increased by 3.83%, i.e. by PLN 15.17 million, and their amount shown as at the end of December 2022 was PLN 395.79 million. As at the end of December 2022, the solvency ratio of the SKOKs was 4.22% and was lower than the 5% threshold required by law. Compared to the balance as at the end of 2021, assets held by the SKOKs increased by 0.29%, i.e. by PLN 28.83 million, to PLN 10,063.64 million.

---

[39] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2021), Warsaw, 2022, p. 24

[40] Jednostkowe sprawozdanie finansowe GPW w Warszawie za rok zakończony 31 grudnia 2022 r. (Separate financial statements of Warsaw Stock Exchange for the financial year ended on 31 December 2022), Warsaw, 2023, p. 12, at: https://www.gpw.pl/pl-ri-raporty-okresowe?geri_id=996&title=Jednostkowy+raport+roczny+GPW+za+2022+rok+&ph_main_01_start=show

[41] Data from Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji *ustawy z dnia 1 marca 2018 r.o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2022 roku (Report of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2022), pp. 21-22, at: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej

59. The gross loan and credit portfolio increased by 2.03%, i.e. by PLN 156.16 million, to PLN 7,692.30 million, while the value of deposits decreased by 1.75%, i.e. by PLN 162.16 million, to PLN 9.283.42 million.

60. The economic and financial situation of the SKOKs varies. The operation of some of the SKOKs is secure, while the economic and financial situation of the others is difficult and requires remedial or restructuring measures. As at the end of December 2022, 10 SKOKs were required to implement a rehabilitation programme.

Currency exchange office operators

61. In accordance with the *Act of 27 July 2002 – Foreign Exchange Law*, currency exchange activity is regulated business consisting in the purchase and sale of foreign exchange values and intermediation in their purchase and sale. Currency exchange, as regulated business within the meaning of the provisions of the *Act of 6 March 2018 – Economic Operators' Law* (Journal of Laws of 2023, item 221), requires an entry in the register of currency exchange office operators, maintained by the President of the National Bank of Poland.

62. As at 31 December 2022, the register of currency exchange office operators included 2,352 entities operating 4,577 currency exchange offices, with 280 currency exchange offices with suspended operation.

63. In 2022, 547 inspections were carried out at 480 currency exchange office operators. The inspections covered 743 currency exchange offices. Irregularities in the field of counteracting money laundering and financing of terrorism were found in the course of 98 inspections and concerned 100 operators and 141 currency exchange offices. In 2022, 30 decisions on the imposition of administrative penalties were issued in connection with ascertaining non-compliance with the obligations arising from the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. The total value of the fines imposed under the decisions issued in 2022 was PLN 280,000[42].

Other entities providing currency exchange services or currency exchange intermediation services

Online currency exchange platforms

64. The operation of entities conducting currency exchange via the Internet and entities providing services consisting in collecting and matching currency conversion orders from various customers and organising/enabling such exchange between them is regulated by the *Act of 6 March 2018 – Economic Operators' Law*.

65. Online currency exchange platforms pose strong competition on the market for traditional currency exchange offices due to measurable benefits they offer, such as speed of the transaction, time savings, convenience, and attractive rates.

66. In 2021, Currency One S.A., the leading company on the online currency exchange market, operating Walutomat and InternetowyKantor.pl, recorded a turnover of approx. PLN 60 billion (compared to PLN 45-55 billion in 2020). This was mainly due to the situation on

[42] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2021 roku (Report of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2021), pp. 25-26, Warsaw, 2022

the markets caused by significant fluctuations in exchange rates related to, among others, the COVID-19 pandemic, as well as the development of the websites and new services introduced for customers. Approximately 47% of people aged 30-45 exchanged currencies online. At the same time, the number of transactions and the number of foreign transfers increased by 6% and 183%, respectively (in 2020, an increase of 62% compared to 2019 was recorded).[43]. According to data provided by Currency One S.A., the operator of Walutomat.pl and InternetowyKantor.pl online currency exchange websites, in 2022, its overall turnover and the number of new customer registrations increased by 46% and 51%, respectively, which proves the established position of online currency exchange platforms[44].

Activity of cryptocurrency trading facilities[45]

67. Cryptocurrency trading facilities, as entities conducting business involving cryptocurrencies, provide their services both on the Internet and in physical outlets. These entities 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. Cryptocurrency exchanges offer a wider range of services. Buy and sell transactions involving cryptocurrency units can be concluded with a cryptocurrency exchange, as well as – based on matching buy and sell offers of its customers – between their different users. They also offer their customers management of electronic portfolios on their behalf.

68. According to information published at https://gieldykryptowalut.pl/najwieksze-gieldy-i-kantory kryptowalut/ (access on 29 August 2023), at least 32 cryptocurrency trading facilities and 45 cryptocurrency exchanges rendered their services online in Polish. These entities may be considered obligated institutions referred to in Article 2(1)(12) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*.

69. The number of Bitcoin ATMs in Poland (but also worldwide) is constantly growing. The high rate of the growth in the number of these devices shows that there are more and more people interested in a quick exchange of cryptocurrencies, e.g. for cash (despite high commissions on such transactions). According to coinatmradar.com, as at the end of December 2014, there were 301 Bitcoin ATMs in the world, while as at 30 June 2023, their number was 35,890.

70. According to the information posted on the website of the Regional Revenue Administration Office in Katowice, maintaining the register of virtual currency service providers, this register included 914 entities as at 28 August 2023[46].

[43] Podsumowanie 2021 r. w kantorach, Currency One oraz prognozy na 2022 r. (Summary of 2021 in currency exchange offices, Currency One and forecasts for 2022) at: https://currency-one.com/podsumowanie-rynku-kantorow-raport-i-infografika, pp. 19-21.; Podsumowanie 2021 r. w kantorach, Currency One 2021 r. (Summary of 2021 in currency exchange offices, Currency One 2021) at: https://currency-one.com/podsumowanie-roku-2020-w-kantorach

[44] https://currency-one.com/podsumowanie-rynku-kantorow-internetowych-2022

[45] In the literature and in the media, cryptocurrency trading facilities are also referred to as "cryptocurrency exchange offices".

[46] https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych

Financial institutions, branches of financial institutions

71. Pursuant to the *Banking Law Act* a financial institution means a financial institution referred to in Article 4(1)(26) of *Regulation (EU) No 575/2013 of the European Parliament and of the Council*, 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 access to the activity of credit institutions 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 concept 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, 5.12.2007, p. 1)[47] and asset management companies, but excluding insurance holding companies and mixed-activity insurance holding companies as defined in Article 212(1)(f) and (g), respectively, 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).

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

- undertakings whose primary activity includes the performance of at least one of the following types of activities: granting loans, leasing, payment services, issuing media of exchange such as cheques, granting guarantees, trading in certain financial instruments (cheques, bills of exchange, certificates of deposit, foreign currencies, options and futures contracts, swaps, securities), participation in the issuance of securities, advice on capital structure or industrial strategy and ownership transformations, intermediation on the money market, investment portfolio management and consultancy in this area, safekeeping and administration of securities, and the issuance of electronic money,
- payment institutions and holding companies of financial institutions (except for holding companies of insurance institutions),
- lending institutions operating under the *Act of 12 May 2011 on consumer credit* (Journal of Laws of 2023, item 1028). According to information published on the KNF website (as checked on 26 April 2022), the register listed 528 lending institutions[48].

73. According to the Statistics Poland information of 19 March 2023 on entities entered in the National Official Business Register REGON, as at the end of 2022, the register listed 614 (compared to 633 in 2021 and 642 in 2020) economic entities reporting business involving financial leasing – Polish Classification of Activities (PKD) 64.91.Z. According to the

[47] The Directive concerned was repealed and replaced by *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 and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.*

[48] https://rpkip.knf.gov.pl/, read on 26.04.2022

aforementioned Statistics Poland data, the greatest number of companies in this industry were registered in the Mazowieckie Voivodeship – 219 (compared to 227 in 2021 and 225 in 2020).

74. According to the Statistics Poland data contained in quarterly information on national economy entities, as at 31 December 2022, the National Official Business Register REGON listed (excluding natural persons running solely private farms) a total of 8,441 (compared to 8,876 in 2021) entities reporting the business defined by the Polish Classification of Activities (PKD) code – 64.99Z, i.e. other financial service activities, except insurance and pension funding not elsewhere classified (this subclass includes, among others, factoring services)[49].

75. Apart from the aforementioned financial institutions, Krajowy Depozyt Papierów Wartościowych S.A. (KDPW S.A.) and the company commissioned to carry out the activities referred to in Article 48(1)(1) of the *Act of 29 July 2005 on trading in financial instruments* are also obligated institutions in so far as they keep securities accounts or omnibus accounts.

2.2. NON-FINANCIAL MARKET

76. *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 offences and imposed obligations on the financial sector only. The 2001 amendment to this Directive extended its scope both in terms of offences and professions as well as areas of activities covered by the provisions on counteracting money laundering and financing of terrorism. It was proposed to extend the scope of criminal offences covered by this Directive to include a wide range of non-financial activities and professions susceptible to money laundering.

77. Outside the financial market, there are many categories of entities offering various types of services and products that can be used for criminal purposes, including money laundering and financing of terrorism. Many of them are obligated institutions within the meaning of the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. In accordance with the aforementioned Act, all these obligated institutions from outside the financial sector have specific obligations that must be unconditionally fulfilled in the manner defined in its provisions.

Gambling

78. The operation of the gambling market is regulated by the Gambling Act of 19 November 2009 (Journal of Laws of 2023, item 227) and secondary legislation thereto. Pursuant to the aforementioned Act, gambling games include games of chance, betting, card games and games on gaming machines.

79. As at 12 January 2023, 51 licences for operating casinos, specifying the location of each of them, had been issued. As at 1 March 2023, there were a total of 23 entities authorised by the Minister of Finance to organise betting and operating lawfully on the betting market. A permit issued by the Minister of Finance for organising betting in permanent outlets was held by 10 entities, while 22 entities held this Minister's permit for organising and operating betting via the Internet. One entity was authorised to organise and conduct other types of gambling via

[49]https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2021,7,9.html

the Internet, such as games on gaming machines, card games, cylindrical games, dice games (totalcasino.pl) as well as numbers games and cash lotteries (gry.lotto.pl).

80. According to the information posted on the website of the Ministry of Finance, in 2021, the National Revenue Administration recorded an increase in the total value of revenue by 52.5%, i.e. by PLN 14.18 billion, compared to 2020. The greatest increase was recorded with respect to casino games organised on the Internet (by 108.9%, i.e. PLN 9.56 billion) and betting (by 46%, i.e. PLN 3.34 billion). At the same time, a decrease in revenue generated by the land-based casino sector was recorded (by 1.1%, i.e. PLN 0.05 billion)[50].

81. The amount of gaming tax in 2020 - 2022 is presented in the table below[51].

Table 4 – Tax on gambling by game type in 2020 - 2022 (in PLN thousand)

Game type	2020	2021	2022
Games covered by state monopoly:	1,182,818	1,499,511	1,893,853
- Draw-based games	765,614	822,034	900,753
- Cash lotteries	219,420	282,638	337,780
- Games on gaming machines	34,323	45,714	118,407
- Online casino games	163,461	349,125	536,913
Casino games	319,251	311,671	546,033
Betting	874,000	1,284,238	1,475,638
Audio-text lotteries	10,415	14,435	21,765
Raffles	4	3	1

Postal operators

82. In accordance with the *Act of 23 November 2012 – Postal Law* (Journal of Laws of 2023, item 1640), a postal operator is an economic operator authorised to perform postal activity under 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 obliged to provide postal services. In accordance with the decision of the President of the Office of Electronic Communications, Poczta Polska is the operator designated to provide universal postal services in 2016-2025.

83. Postal operators have been covered by the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in order to ensure the tightness of the system for counteracting money laundering and financing of terrorism, as they provide, among others, postal money order services, both within Poland and transnationally.

84. The postal service market consists of the following main segments: courier services, universal services, services falling within the scope of universal services, and other postal services.

85. In 2022, postal operators provided a total of 1,956.7 million postal services, which, compared to 2021, represents an increase by 21.6 million services, i.e. 1.1%. This increase was due to an increase in the volume of courier shipments by 15.2%. As regards the volume of parcel post and letter post, declines by 5.0% and 8.2%, respectively, were recorded.

[50] https://www.gov.pl/web/kas/sytuacja-na-rynku-gier-hazardowych-online, access on 27.04.2022
[51] https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/sprawozdawczosc/ access on 21.08.2023

86. As at the end of 2022, there were 274 postal operators, which represents a decrease compared to 2021 (300 postal operators) and 2020 (291 postal operators).

87. As at the end of 2022, the total value of the Polish postal services market amounted to PLN 14,363.9 million. Thus compared to the previous year, the total amount of nominal revenue from postal services rendered by operators on the Polish market increased by PLN 1,473.0 million, which translates into an annual growth rate of 11.4%. As in previous years, this increase was mainly due to the increase in revenue from courier services, resulting from the consistently growing volumes of shipments containing goods purchased by consumers as part of e-commerce transactions. In 2022, a further decline (by 17.3%) in revenue from parcel post was recorded. As for other product categories, increases were recorded, including with respect to letter post (by 3.6%).

88. In 2022, postal services were provided in 30,237 post offices, including 7,620 offices of the designated operator and 22,617 offices of alternative operators.

Liberal legal professions

89. Liberal legal professions are professions of public trust that are pursued in the scope and manner described in specific provisions. They are pursued in the form of specific type of services, most often intangible ones, with specific liberal profession – client relationships. The aim of the activities of individuals practicing legal professions is to ensure the security of legal transactions.

90. Pursuant to the Code of Commercial Partnerships and Companies, liberal professions include legal or similar professions, such as an attorney, tax advisor, notary, legal counsel.

91. According to the National Council of Notaries information, as at 19 March 2023, the profession of notary was practised by 3,777 individuals (compared to 3,644 ones in 2021)[52].

92. According to the information contained in the National Register of Attorneys and Attorney Trainees kept by the Polish Bar Association, as at 19 March 2023, there were 30,113 attorneys (compared to 28,637 ones in 2021) practicing their profession[53], and 174 foreign lawyers providing legal assistance[54] (compared to 154 ones practising their profession in 2021).

93. According to the information contained in the search engine of legal counsels, made available by the National Chamber of Legal Counsels, as at 19 March 2023, there were 51,811 legal counsels[55] (compared to 50,220 ones in 2021).

94. The list of tax advisors included, as at 19 March 2023, 8,893 individuals practising this profession (compared to 8,849 ones in 2021)[56].

Expert auditors

95. Expert auditors practise their profession in accordance with the *Act of 11 May 2017 on expert auditors, audit firms and public supervision* (consolidated text: Journal of Laws of 2023, item 1015). These are financial audit activities and assurance services other than financial audit

[52] https://krn.org.pl/
[53] https://rejestradwokatow.pl/adwokat
[54] http://rejestradwokatow.pl/prawnikzagraniczny/ewidencja
[55] https://rejestrradcow.pl/Home,
[56] https://kidp.pl/doradcy.php

activities, not reserved for expert auditors, as well as related services. A expert auditor may practise their profession as: a natural person conducting business activity in their name and on their account or a partner of an audit firm, or a natural person in an employment relationship with an audit firm, or a natural person (including a person conducting business activity in a scope other than that mentioned above) that has concluded a civil law contract with an audit company.

96. In accordance with information from the register of expert auditors kept by the National Council of Expert Auditors, as at 20 March 2023, there were 5,024 expert auditors[57] (compared to 5,204 in 2021) and 1,248 audit firms[58] (compared to 1,353 in 2021).

Bookkeeping services

97. In accordance with Article 76a(1) of the *Accounting Act of 29 September 1994* (Journal of Laws of 2023, item 120), the provision of bookkeeping services is a business activity within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, consisting in the provision of bookkeeping services, determining and checking the balance of assets and liabilities, valuation of assets and liabilities, determining one's profit or loss, preparing financial statements, and collecting and storing accounting evidence and other documentation provided for in the aforementioned Act.

98. According to the Statistics Poland data contained in the quarterly information on national economy entities, as at 31 December 2022, the National Official Business Register REGON (excluding natural persons running solely private farms) included 62,911 entities reporting the activity defined by the Polish Classification of Activities (PKD) code – 6920Z, i.e. accounting and bookkeeping services and tax consultancy.

Foundations and associations

99. In accordance with the *Act of 6 April 1984 on foundations* (Journal of Laws of 2023, item 166), a foundation is a legal form of a non-governmental organisation in which capital allocated for a specific purpose plays an important role. A foundation may be established to implement socially or economically useful objectives in line with the fundamental interests of the Republic of Poland, that include, in particular: health care, development of the economy and science, education and upbringing, culture and arts, social care and welfare, environmental protection and preservation of monuments.

100. An association is a basic organisational and legal form in which one of the most important citizen rights enshrined in the Constitution – i.e. the right to freedom of association and joint activities – is exercised. In accordance with Article 2(1) of the *Act of 7 April 1989 – Law on Associations* (consolidated text: Journal of Laws of 2020, item 2261), it is a "voluntary, self-governing, sustainable non-profit-making association".

101. Only those foundations and associations that have legal personality are obligated institutions in so far as they accept or make cash payments with a value equal to or greater than the equivalent of EUR 10,000, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other.

[57] https://www.pibr.org.pl/pl/search/auditor?search
[58] https://strefa.pana.gov.pl/wyszukiwarka/

102. According to information obtained in accordance with Article 14(4) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* from poviat governors, voivodeship governors and ministers, a total of 15 obligated institutions were identified (as at 31 December 2022)[59]. Among the obligated institutions supervised by the aforementioned bodies, there were two associations and seven foundations. In the case of six organisations the competent body did not specify the legal form of the supervised entity. Based on the information provided, 91% of poviat governors assessed human and financial resources held as sufficient to carry out tasks in the field of counteracting money laundering and financing of terrorism, while the remaining 9% of them assessed their human and financial resources as insufficient. In the vast majority of poviat governors' offices, tasks related to the implementation of obligations related to counteracting money laundering and financing of terrorism were carried out by one or two employees, and the costs of these activities included primarily the employee's salary as well as the costs of postage and stationery consumption. Depending on the inclusion of the employee's tasks in the work regulations in a particular poviat governor's office, these costs ranged from several hundred PLN to PLN 14,000 per annum. In the vast majority of poviat governor's offices, one or two training courses on counteracting money laundering and financing of terrorism were conducted in 2022.

103. According to information obtained in accordance with Article 14(4) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* from poviat governors, voivodeship governors and ministers, a total of 18 obligated institutions were identified (as at 31 December 2022). The obligated institutions supervised by the aforementioned bodies included nine associations and nine foundations.

104. According to the information contained in the report on the research by the Klon/Jawor Association, the COVID-19 pandemic affected the operation of non-governmental organisations to varying degrees. At the turn of 2021, more than half of these organisations were able to conduct most or all of their activities (often in a modified form, e.g. remotely). At the same time, over 40% of associations and foundations had most of their activities suspended, mainly due to restricted contact with the beneficiaries of their activities. Organisations that ceased their activities for the aforementioned reason included both those that were affected by the consequences of the restrictions and those that decided themselves not to expose their beneficiaries to the risk of contact with the COVID-19 virus[60].

Real estate market

105. Trade in real estate in Poland is regulated by the *Act of 21 August 1997 on real estate management* (Journal of Laws of 2023, item 344). Pursuant to the aforementioned Act, real estate may be traded, in particular, it may be: sold, exchanged or relinquished, put into perpetual usufruct, rented or leased, let, put into permanent management, as well as encumbered with limited property rights, contributed in kind to companies, transferred to equip state-owned enterprises being established and as assets of foundations being established.

[59] The information provided by the ministers, poviat governors and voivodeship governors was based on their knowledge.
[60] Rok w pandemii, Raport z badań organizacji pozarządowych 2020/2021, Stowarzyszenie Klon/Jawor, Warsaw, March 2021, pp. 14, 16.

106. Real estate brokers are obligated institutions within the meaning of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*.

107. According to the Statistics Poland data contained in the quarterly information on national economy entities, as at 31 December 2022, the National Official Business Register REGON (excluding natural persons running solely private farms) included a total of 21,878 entities (compared to 22,091 ones in 2021) reporting the activity defined by the Polish Classification of Activities (PKD) code – 6831Z, i.e. intermediary services in the real estate trading.

Other market segments

Art market

108. In accordance with the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, obligated institutions include economic operators within the meaning of the *Act – Economic Operators' Law*, conducting business consisting in:

- trade in or intermediation in the trade in works of art, collectibles and antiques within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services* (Journal of Laws of 2023, item 1570), also where such activity is carried out in art galleries or auction houses, or using a free port, understood as a zone or room where goods are treated as not located within the customs territories of the Member States or third countries, including the use of a duty-free zone;
- storage of works of art, collectibles and antiques, within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services* (Journal of Laws of 2023, item 1570), where such activity is carried out using a free port referred to above

- with respect to transactions with a value equal to or greater than the equivalent of EUR 10,000, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other.

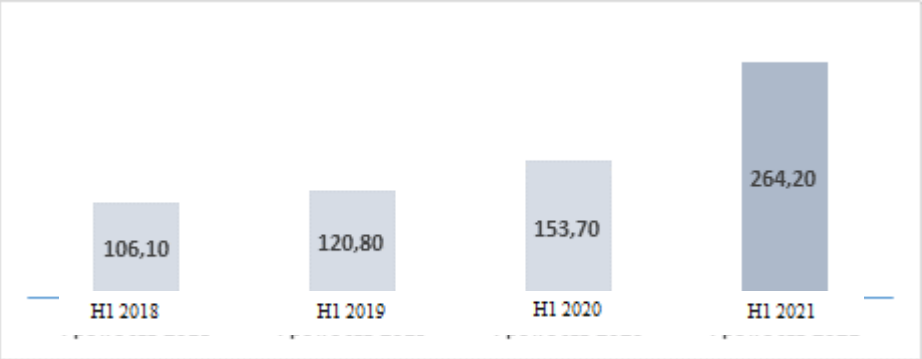
109. According to the Statistics Poland news release of 25 May 2022, in 2021, exhibitions were organised by 313 art galleries (compared to 307 in 2020). Art galleries organised in Poland a total of 3,054 exhibitions (677 more than in 2020), including 2,682 national exhibitions, 217 international exhibitions and 155 exhibitions held abroad. Due to the ongoing COVID-19 pandemic in Poland, art galleries extended their activities on the Internet – 46.6% of galleries held 755 online exhibitions. According to the Statistics Poland news release of 25 April 2023, in 2022, 310 art galleries operating at that time organised 3.5 thousand exhibitions in Poland for 3 million visitors. Compared to 2021, the number of exhibitions held in Poland increased, but the number of visitors decreased by 13.8%[61].

110. A significant part of art galleries belonged to the public sector (63.3%) and as such they were organised by local government units. The remaining art galleries were owned by the private sector, including natural persons and non-governmental organisations. Painting

[61] https://stat.gov.pl/obszary-tematyczne/kultura-turystyka-sport/kultura/dzialalnosc-galerii-sztuki-w-2022-roku,10,6.html

collections accounted for the largest part of the own collections of state-owned galleries and galleries owned by local government units (40.9%)[62].

Chart 4. Turnover on the art market in Poland in the first halves of 2018-2021 (in PLN million)



111. The private banking offer includes, among others, art banking, encompassing professional advice on collecting works of art. However, in Poland, the use of a non-financial service such as art banking is not yet as widespread as in the case of foreign institutions. The banks' offer is limited to simple management of the client's assets and alternative investments. Polish art banking lacks, among others, loans using works of art as collateral, loans for the purchase of works of art or professional advice on the art market. The art banking offer in the Polish private banking offer mainly includes paintings, while in other countries, it also covers sculptures, photographs, posters and comic book boards. In Poland, art banking is not yet popular as a form of capital investment.

Safe deposit boxes

112. Safe deposit boxes are made available by banks, in accordance with the provisions of the *Banking Law Act*, provided that banks perform such activities, as well as by economic operators operating under the provisions of the *Act of 6 March 2018 – Economic Operators' Law*. Economic operators conducting their business under the provisions of the aforementioned Act, in so far as they conduct business consisting in making safe deposit boxes available, as well as branches of foreign economic operators conducting such business 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 financing of terrorism*.[63]

[62]https://stat.gov.pl/obszary-tematyczne/kultura-turystyka-sport/kultura/rynek-dziel-sztuki-i-antykow-w-2021-roku,17,6.html

[63] Offers from at least a dozen non-bank entities offering their services in this area can be found on the Internet.

3. DESCRIPTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1. MONEY LAUNDERING

113. Initially, money laundering was understood as introducing money originating from criminal activities into circulation through business activities (e.g. through ordinary 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 proceeds from a prohibited act, including aiding in its commitment, attempting its commitment 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)[64] 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.

114. Money laundering offences are also described in FATF Recommendation[65] 3, where it is indicated that: "Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences".

115. The first Polish legal regulations related to combating money laundering were enacted at the beginning of the 1990s. These 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*

[64] The Convention was ratified by Poland on 8 August 2007 and entered into force on 1 May 2008.
[65] Recommendations of the Financial Action Task Force on Money Laundering were issued in April 1990 and were most recently updated in October 2021, link: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html,

crime are deposited with a bank and when 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 the NBP organisational units to perform activities aimed at concealing the origin of funds from or related to crime.*

116. The definition of the offence of money laundering and sanctions for committing this offence were defined for the first time in the Polish law in the *Act of 12 October 1994 on the protection of economic transactions and amendment to certain provisions of the criminal law* (Journal of Laws of 126 item 615). This Act identifies a narrow range of possible predicate offences[66], related to organised crime. Money laundering in the first version of Article 299 of the *Act of 6 June 1997 – Penal Code* (Journal of Laws of 2022, item 1138) was described in a similar way.

117. An interesting definition of money laundering was introduced by the *Act of 5 March 2004 amending the Act on counteracting the introduction to financial transactions of assets derived from illegal or undisclosed sources and on counteracting the financing of terrorism and amending certain acts* (Journal of Laws No. 62, item 577), but it was not directly related to the content of the provision of the Penal Code in force at that time, penalising money laundering (Article 299 of the Penal Code). The aforementioned Act indicated that the introduction of assets originating from illegal or undisclosed sources into economic transactions should be understood as "an intentional act consisting in:

(a) the conversion or transfer of assets[67] derived from criminal activity or from participation in such activity, for the purpose of concealing or disguising the illicit origin of these assets or of assisting any person who is involved in the commission of such activity to evade the legal consequences of their action;

(b) the concealment or disguise of the true nature, source, location, movement or rights with respect to assets derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of assets derived from criminal activity or from an act of participation in such activity;

(d) association to commit, attempts to commit and aiding or abetting the commission of any of the actions mentioned in subparagraphs (a) to (c);

(e) also where the activities which generated assets derived from illegal or undisclosed sources being introduced to financial transactions were carried out in the territory of another state"[68].

[66] The concept of the predicate offence refers to punishable acts that may give rise to launderable proceeds. 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 that gives rise to proceeds that may be the subject of a money laundering offence.

[67] Defined then as means of payment, securities or foreign exchange values, property rights, and movable and immovable property.

[68] The concept of "introduction to economic transactions of assets derived from illegal or undisclosed sources" was changed by the *Act of 25 June 2009 amending the Act on counteracting the introduction to financial*

118. Thus, the following were identified as the basic money laundering activities:

- conversion of assets,
- their transfer,
- their acquisition,
- taking possession thereof,
- their use.

119. The aforementioned activities were linked to five fundamental rules:

(1) The activities concern or are to concern assets derived "from criminal activity or from participation in such activity"

(2) The perpetrator is aware of the illegal origin of the aforementioned assets.

(3) The purpose of the aforementioned activities is to conceal or disguise the illegal origin of assets or their nature, as well as their source, place of storage, disposition, and the fact of their movement.

(4) Activities undertaken for the aforementioned purpose also include: collaboration, attempting to commit them, aiding or abetting.

(5) The predicate offence for money laundering may be committed both in and outside the territory of Poland.

120. Currently, in the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the concept of money laundering is defined by reference to the content of Article 299 of the Penal Code. Pursuant to the aforementioned provision penalising this crime, money laundering should be understood as:

- accepting, possessing, using, handing over 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 assets,
- undertaking other activities that may prevent or significantly hinder the determination of the criminal origin or location of the aforementioned assets, their detection, seizure or forfeiture.

3.2. FINANCING OF TERRORISM

121. Counteracting money laundering is closely linked with combating the financing of terrorism. This relationship is based, in particular, on two facts:

- terrorist activities are often financed with proceeds from illegal activities,

---

transactions of assets derived from illegal or undisclosed sources and on counteracting the financing of terrorism 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 sentence common for all subparagraphs of this definition.

- similar methods (including ways of transferring funds) are used to finance terrorism as in the case of money laundering.

122. There are various definitions of terrorism, to which numerous scientific studies have been devoted. This is mainly due to the fact that terrorism is commonly identified with the means used, i.e. violence on a relatively large scale. For this reason, this concept is often defined as a specific method of operation rather than a separate, comprehensive political phenomenon[69]. Basically, most definitions of terrorism have certain common elements. These are:

- perpetrators of terrorist acts: extremists,
- the method they use: violence or the threat of using violence,
- addressees of terrorist acts: society or its part, the authorities of the country/countries concerned, international institutions and organisations;
- indirect objective of perpetrators: to intimidate the addressee,
- the main objective of perpetrators: to obtain political concession.

123. Unlike defining terrorism, the concept of financing of terrorism is easier to formulate. In fact, most of its definitions resemble those 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» means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA"[70].

124. *The Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, implementing the provisions of the aforementioned Directive, defines financing of terrorism by reference to Article 165a of the Penal Code.

125. The current wording of Article 165a of the *Penal Code* describes in detail the conduct defined as financing of terrorism. In accordance with this provision, financing of terrorism includes:

- raising, transferring or offering legal tenders, financial instruments, securities, foreign exchange values, property rights or other movable or immovable property to finance a terrorist offence[71] or an offence referred to in Article 120, Article 121, Article 136,

[69] Damian Szlachter, Walka z terroryzmem w Unii Europejskiej – nowy impuls, publishing house: Adam Marszałek, Warsaw, 2007, p. 22.
[70] 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 means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism".
[71] A terrorist offence is defined in Article 115(20) of the Penal Code.

Article 166, Article 167, Article 171, Article 252, Article 255a or Article 259a of the *Penal Code*,

- 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 aforementioned group, association or person.

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

4. SYSTEM FOR COUNTERACTING MONEY LAUNDERING AND FINANCING OF TERRORISM

4.1. APPLICABLE REGULATIONS

127. *The Act of 1 March 2018 on counteracting money laundering and financing of terrorism* is the key legal act relating to counteracting money laundering and terrorism financing. The aforementioned Act implements the provisions of *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), hereinafter referred to as Directive 2015/849, implements *Directive (EU) 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 purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU* (OJ L 156, 19.06.2018, p. 43). First of all, it defines the tasks and powers of the GIFI, as well as the operation of the Financial Security Committee, the rules for the GIFI's collaboration with its cooperating units, and the obligations of obligated institutions.

128. The aforementioned Act served as the grounds for issuing and enacting regulations[72] specifying the following issues:

- determination of a list of national public positions and functions that are exposed political positions, having regard to the nature of the tasks performed and their importance to counteracting money laundering and financing of terrorism,
- the method of receiving, handling and storing reports as well as informing about actions that may be taken following report receipt, having regard to the need to ensure adequate protection of reporting persons, including the protection of their personal data,
- the method of and procedure for submitting reports to the Central Register of Beneficial Owners (CRBR), having regard to the need to ensure safe, efficient and reliable reporting,
- the method of preparing and submitting requests, the procedure for filing requests for information to be reported to the CRBR and making this information available, and the deadlines for making information available, having regard to the need to ensure quick, reliable and secure access to information from the Register,
- the ability to designate a body of the National Revenue Administration (KAS) to perform the tasks of the body competent in the CRBR matters, specifying the scope

[72] Statutory delegations referred to in Article 46c, Article 53a(4), Article 62, Article 71, Article 71a, Article 78(3), Article 79(3), Article 80(3), Article 84(4), Article 85(4), Article 94, Article 129ka, Article 129l, Article 129wa(2), Article 129x and Article 134(2) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism.*

of these tasks, having regard to the technical and organisational preparation of the office serving this body,

- the method of preparing and transmitting: information on the accepted payment or withdrawal of funds equivalent to EUR 15,000, the transfer of funds equivalent to more than EUR 15,000, the form identifying the obligated institution, as well as the mode of their transfer (taking into account the need for efficient, reliable and safe transmission),
- the method of receiving reports regarding actual and potential violations of regulations, the method of handling and storing reports, as well as the method of informing about actions that may be taken following report receipt, having regard to the need to ensure adequate protection, including the protection of personal data, of reporting persons or persons who have allegedly violated regulations on counteracting money laundering and financing of terrorism,
- the method of and procedure for submitting requests for entry into the register of trust or company service providers, amending the entry in this register and removal from this register, as well as notices of the suspension of business activity, having regard to the need to ensure safe and efficient submission of these requests and notifications,
- designation of a body of the National Revenue Administration (KAS) to perform the tasks of the body competent for keeping the register of trust or company service providers, specifying the scope of these tasks, having regard to the technical and organisational preparation of the office serving this body,
- the method of and procedure for submitting requests for entry into the register of virtual currency service providers, amending the entry in this register and removal from this register, as well as notices of the suspension of business activity, having regard to the need to ensure safe and efficient submission of these requests and notifications,
- designation of a body of the National Revenue Administration (KAS) to perform the tasks of the body competent for keeping the register of virtual currency service providers, specifying the scope of these tasks, having regard to the technical and organisational capacities of the office serving this body,
- defining the template of the controller's official ID card and the procedure for its issuance and replacement, having regard to the need to ensure the controller's identification and their adequate protection.

129. Besides the aforementioned Act, EU regulations are also of great importance for the operation of the national system for counteracting money laundering and financing of terrorism.

130. *Directive 2005/60/EC* was repealed by *Directive 2015/849* currently in force. A revised framework for counteracting money laundering and financing of terrorism that besides the aforementioned Directive also includes Regulation 2015/847 on information accompanying transfers of funds[73] was adopted. Despite the implementation of new solutions, a proposal for

[73] 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 11, p. 1, as amended). On

a draft amendment to *Directive 2015/849* was submitted on 5 July 2016. In its Explanatory Memorandum, it was pointed out that: "gaps still exist in the oversight of the many financial means used by terrorists, from cash and trade in cultural artefacts to virtual currencies and anonymous pre-paid cards. Action to amend the Directive and tighten the European AML/CFT system was triggered primarily the analyses performed after the terrorist attacks in France and Belgium to determine the methods of their financing, as well as the information disclosed in connection with the Panama Papers scandal. The provisions of the amendment to the Directive were to cover two strands of action: tracing terrorists through financial operations and preventing them from moving funds or other assets as well as disrupting the sources of revenue used by terrorist organisations, by targeting their capacity to raise funds. The purpose of *Directive (EU) 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 purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU* is to prevent the large-scale concealment of funds which can hinder the effective fight against financial crime, and to ensure enhanced corporate transparency so that true beneficial owners of companies or other legal arrangements cannot hide behind undisclosed identities"[74].

131. On 20 July 2021, the European Commission presented a legislative package aimed at strengthening the anti-money laundering and anti-terrorist financing framework. Its components include the creation of the Authority for Anti-Money Laundering and Countering Financing of Terrorism (AMLA). The Regulation grants AMLA the right to directly supervise selected obligated institutions – high-risk financial institutions operating in the territory of many Member States or requiring immediate corrective actions that cannot be effectively dealt with by the national supervisory authority. The assessment of obligated institutions in terms of including them on the list of high-risk institutions is to be carried out every 3 years in accordance with a uniform methodology developed by the AMLA. The AMLA will conduct periodic reviews of national supervisory authorities to verify whether they have sufficient resources and powers to effectively perform their functions. On 3 June 2021, the provisions of *Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005* (OJ L 284/6, 12.11.2018) and implementing regulations thereto establishing templates for certain forms as well as technical rules for the effective exchange of information under this Regulation entered into force. The new regulations extend the obligations of, among others, persons carrying cash[75] across the border and areas of control carried out by border services. A person carrying EUR 10,000 or amounts above this limit is obliged to report this fact during border control, which involves submitting a declaration to the customs and tax control authorities or border guard authorities.

9 June 2023, *REGULATION (EU) 2023/1113 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/ 849* was published in the Official Journal of European Union.

[74]EC Explanatory Memorandum of 5 July 2016, p. 3, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016PC0450\&from=EN, access on 25.04.2020).

[75] Within the meaning of this Regulation *"cash" means: currency, bearer-negotiable instruments, commodities used as highly-liquid stores of value, and prepaid cards.*

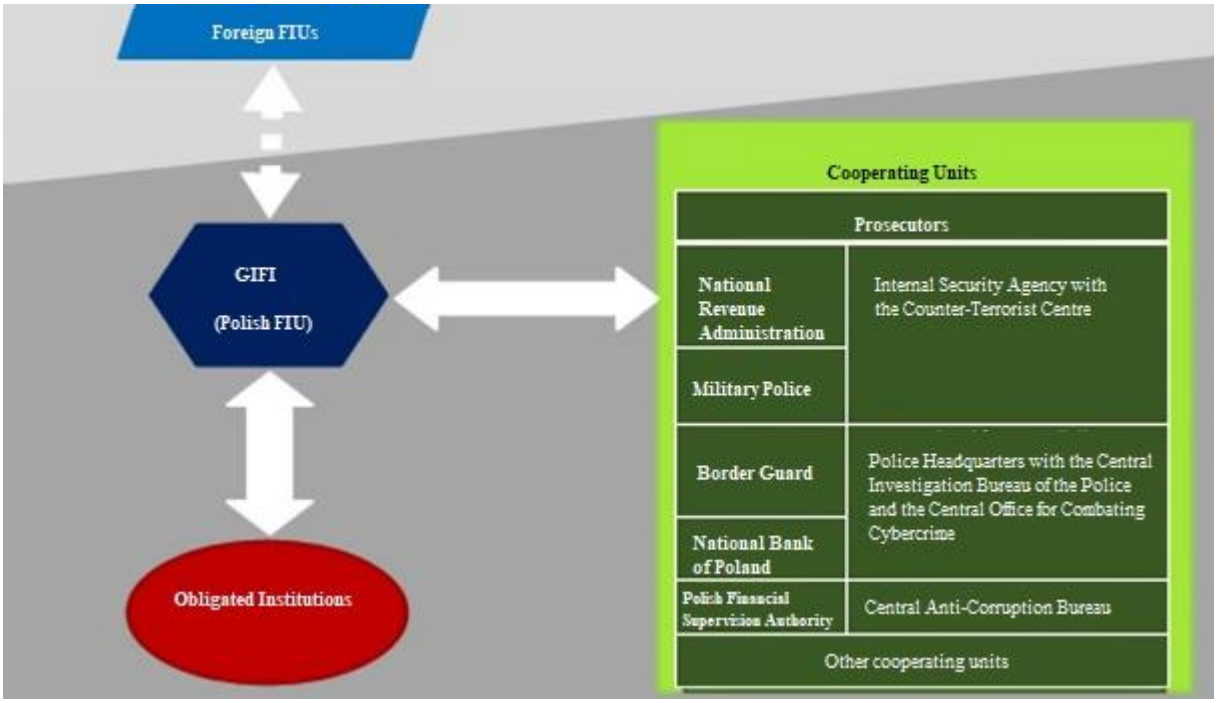
133. The operation of the national system for counteracting money laundering and financing of terrorism is also affected by national legal acts specifying the powers and tasks of particular public administration bodies that combat crime or supervise the activity of obligated institutions.

4.2. SYSTEM FOR COUNTERACTING MONEY LAUNDERING AND FINANCING OF TERRORISM IN POLAND

134. The Polish system for counteracting money laundering and financing of terrorism consists of:

- the GIFI,
- obligated institutions,
- cooperating units.

Diagram 2. Polish system for counteracting money laundering and financing of terrorism



4.2.1. General Inspector of Financial Information

135. The General Inspector of Financial Information (GIFI) plays a leading role in the Polish system for counteracting money laundering and financing of terrorism.

136. Pursuant to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the government administration bodies competent for counteracting money laundering and terrorist financing include:

- the minister competent for public finance as the chief financial information authority,
- the General Inspector of Financial Information.

137. The GIFI is appointed and dismissed by the Prime Minister at the request of the minister competent for public finance, following consultation with the minister – member of the Council of Ministers competent for the coordination of the operation of secret intelligence services, if appointed by the Prime Minister. The GIFI may be a secretary or undersecretary of state in the office supporting the minister competent for public finance. The range of activities of a secretary or undersecretary of state stipulated in Article 37(2) of the *Act of 8 August 1996 on the Council of Ministers* (Journal of Laws of 2022, item 1188) does not cover the tasks of the General Inspector of Financial Information performed pursuant to the provisions on counteracting money laundering and financing of terrorism. The term of office of the General Inspector of Financial Information begins on the day of its appointment, lasts 6 years and may not be held by the same person for more than two terms.

138. The GIFI carries out the tasks of a financial intelligence unit within the meaning of *Directive 2015/849*, assisted by an organisational unit separated in the office supporting the minister competent for public finance in order to ensure the proper implementation of the GIFI's tasks.

139. The GIFI performs its tasks with the support of the Department of Financial Information of the Ministry of Finance, acting with it as the Polish financial intelligence unit.

140. The minister competent for public finance provides the headquarters, legal, organisational and technical services for the GIFI, and also bears financial expenses from the state budget related to the GIFI's operation and salary.

141. The GIFI is the administrator of the ICT system used to counteract money laundering and financing of terrorism.

142. The GIFI's tasks include taking action to counteract money laundering and financing of terrorism, in particular:

- analysing information related to assets suspected by the General Inspector to be related to a money laundering or terrorism financing offence,
- suspending transactions or blocking banks accounts,
- requesting submission of information on transactions and disclosure thereof,
- providing authorised authorities with information and documents justifying the suspicion of committing a crime,
- exchanging information with cooperating units,
- developing the National Assessment of the risk of money laundering and financing of terrorism as well as strategies for counteracting these offences, together with cooperating units and obligated institutions,
- monitoring compliance with the provisions on counteracting money laundering and financing of terrorism,
- issuing decisions on entry into the list of persons and entities towards whom or which specific restrictive measures are applied, or their delisting, and keeping this list,

- cooperation with competent authorities in other countries as well as foreign institutions and international organisations dealing with counteracting money laundering or financing of terrorism,
- exchanging information with foreign financial intelligence units, including maintaining a contact point for the purposes of this exchange,
- imposing administrative penalties referred to in the Act,
- providing knowledge and information relating to the provisions on counteracting money laundering and financing of terrorism in the Public Information Bulletin, on the website of the office supporting the minister competent for public finance,
- processing information in accordance with the procedures specified in the Act,
- initiating other activities to counteract money laundering and financing of terrorism.

143. The GIFI makes available, upon request or *ex officio*, and obtains from foreign financial intelligence units information related to money laundering or financing of terrorism, including information on prohibited acts that may generate assets. The exchange of information with its foreign counterparts, i.e. FIUs, is one of the important tasks of the GIFI, as this information is to be used in the performance of financial intelligence units' tasks defined in the national regulations implementing *Directive 2015/848* and the provisions of international law regulating the principles of operation of financial intelligence units.

144. Besides the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, information with FIUs is exchanged also under the Warsaw Convention. The GIFI may exchange information with the FIUs from countries that have ratified this Convention. The above document, ratified by Poland, provides that FIUs "FIUs exchange, spontaneously or on request and either in accordance with this Convention or in accordance with existing or future memoranda of understanding compatible with this Convention, any accessible information that may be relevant to the processing or analysis of information or, if appropriate, to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved".

145. The currently applicable *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* regulates in detail issues related to the exchange of information with foreign FIUs, in accordance with *Directive 2015/849*. Generally, the provisions of the aforementioned Act indicate that cooperation in this area is based on providing foreign FIUs by the GIFI, on their request or *ex officio*, and obtaining from these units by the GIFI information related to money laundering or financing of terrorism, including information on prohibited acts that may generate assets, as well as information that may be important for detecting or combating terrorism or related organised crime. Information is made available to be used in the performance of financial intelligence units' tasks defined in *Directive 2015/849*, national regulations implementing this Directive or the provisions of international law regulating the principles of operation of financial intelligence units. Information that may be important for detecting or combating terrorism or related organised crime is made available in urgent cases, where the provision of information by other means may prove insufficient for the purposes of combating terrorism or related organised crime. The GIFI makes available the information and documents held to the financial intelligence units of the Member States, while the provision of

the information held by it to the financial intelligence units from non-member states is made on a reciprocity basis, and to the financial intelligence units of the countries that are parties to 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*, drawn up in Warsaw on 16 May 2005 – on the terms set out in this Convention. To information made available to foreign financial intelligence units the provision of Article 99(7) shall not apply, except for the provisions of the *Act of 5 August 2010 on the protection of classified information* (Journal of Laws of 2023, item 756).

146. Furthermore, the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* do not require a bilateral agreement to be signed with a foreign FIU to exchange information[76]. The agreements signed so far remain in force.

147. Statutory regulations also indicate cases in which the GIFI refuses to make information or documents available to a foreign financial intelligence unit or refuses to transfer information or documents to other authorities or financial intelligence units or to use such information or documents for purposes other than those defined in Article 110(2) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, if:

- this unit's request for making information available does not relate to the information referred to in Article 110(1) or is not related to money laundering or financing of terrorism,
- the requested information is protected in accordance with the provisions on the protection of classified information,
- providing the requested information could impede the performance of their tasks by judicial authorities and services or institutions responsible for protecting public order, security of citizens or prosecuting perpetrators of offences or fiscal offences,
- disclosure of the requested information could threaten the security of the state or public order,
- the third country does not guarantee an adequate level of personal data protection.

The occurrence of the circumstances referred to above results in mandatory refusal to provide information to a foreign financial intelligence unit, but such refusal requires substantiation.

148. The aforementioned Act introduced minor differences between the exchange of information with FIUs from EU Member States and the exchange of information with FIUs from other countries. In the first case, the GIFI provides FIUs with information and documents held without verifying whether the principle of reciprocity has been observed[77]. The GIFI has also been obliged to use for this purpose secure communication systems and ICT systems enabling comparison of GIFI data with data held by these units in an anonymous manner, while ensuring the protection of personal data (i.e. the FIU.NET ICT system currently in use and the ma3tch technology[78]). Moreover, the GIFI transfers *ex officio* to the FIU of another EU Member

[76] Such agreement may be signed if the national regulations of the other party so require or if there is a need to specify the procedure and technical conditions for the exchange of information.
[77] The lack of reference to this principle results from the fact that FIUs from EU Member States are obliged to implement the same cooperation rules specified in *Directive 2015/849.*
[78] FIU.NET and ma3tch technology were also used in the previous legal system.

State information concerning this state (e.g. its residents, transactions carried out by institutions established therein), received from obligated institutions, regarding:

- circumstances that may indicate a suspicion of committing a money laundering or terrorism financing offence,
- cases of becoming aware of a reasonable suspicion that a specific transaction or specific assets may be related to money laundering or financing of terrorism,
- notifying the prosecutor of cases of becoming aware of a reasonable suspicion that the assets being the subject of a transaction or deposited in an account originate from an offence other than money laundering or financing of terrorism or from a fiscal offence, or are related to an offence other than money laundering or financing of terrorism or with a fiscal offence.

149. As for FIUs from other non-EU countries, the GIFI provides them with information it holds on a reciprocity basis, whereby the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* clearly indicates that information with FIUs from countries that are parties to the Warsaw Convention is carried out in accordance with the provisions of this Convention[79].

150. To exchange information with FIUs from non-EU countries, the GIFI uses primarily Egmont Secure Web, i.e. the IT system developed within the Egmont Group[80] and used by FIUs being members of this organisation.

151. Besides sharing available information, the GIFI may also obtain additional information (e.g. from obligated institutions or cooperating units) in order to transfer it to a foreign FIU.

152. The provisions of the aforementioned Act also specify the scope of information that should be included in an information request submitted by the GIFI to a foreign FIU, including:

- identification data of suspicious entities[81],

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

[80] Egmont Group was established in 1995 as an informal international organisation, associating FIUs and operating to promote and strengthen international cooperation in combating money laundering and financing of terrorism. As part of its work, basic standards for information exchange between its members were developed and an IT system was launched to accomplish this goal. In 2007, it became a formal international organisation with its own secretariat and staff. As at 31 January 2022, the Egmont Group included FIUs from 167 jurisdictions.

[81] Article 112(1) of the aforementioned Act indicates that the scope of this data should be consistent with the scope of the data specified for obligated institutions applying customer due diligence measures, i.e. in accordance with Article 36(1) of this Act. It should be noted, however, that requests submitted by the GIFI are largely based on information contained in suspicious activity reports (SARs) filed by obligated institutions, which in turn – in accordance with Article 74(3)(2) and Article 86(2) of the aforementioned Act – include only available data of natural persons, legal persons and organisational units without legal personality that are not customers of the obligated institution but are involved in suspicious activities. The similar applies to SARs submitted to the GIFI by cooperating units, that also – in accordance with Article 83(2)(1) of the aforementioned Act – include "available data referred to in Article 36(1) of natural persons, legal persons or organisational units without legal personality, connected with circumstances that may indicate suspicion of committing a money laundering or terrorism financing offence".

- description of circumstances indicating a connection with money laundering or financing of terrorism,
- the intended purpose of using the information.

153. It is also expected that an information request submitted to the GIFI by a foreign FIU should include such information as well. If it fails to meet these requirements or does not sufficiently indicate the connection of the requested information with money laundering or financing of terrorism, the GIFI requests for it to be complemented[82].

154. Upon a justified request of a foreign FIU, the GIFI may allow the information provided by it to be transferred to other authorities or FIUs or to use this information for purposes other than those related to the tasks of financial intelligence units. Likewise, the GIFI may also request a foreign FIU for consent to transfer the information received from this FIU to courts, prosecutors and other cooperating units or other foreign FIUs, or to use this information for purposes other than the performance of its tasks.

155. Furthermore, the GIFI may request that a transaction be suspended or a bank account be blocked at the reasonable request of a foreign FIU "that allows for lending credence to the suspicion of committing a money laundering or terrorism financing offence".

156. The GIFI may share and obtain information as part of cooperation with competent authorities of other countries, foreign institutions and international organisations dealing with counteracting money laundering or financing of terrorism (including EUROPOL) and European supervisory authorities. For this purpose, it may conclude relevant agreements specifying the procedure and technical conditions for providing or obtaining information.

157. As part of cooperation, the GIFI and the KNF – with respect to obligated institutions supervised by each of them – cooperate with the competent authorities of Member States that supervise or control compliance by entities with the provisions on counteracting money laundering and financing of terrorism issued under *Directive 2015/849*, among others by sharing information with these authorities and obtaining information therefrom and acting as contact points for the purposes of this cooperation. The KNF is a contact point for European supervisory authorities in the area of supervision over compliance with the provisions on counteracting money laundering and financing of terrorism issued under *Directive 2015/849*. The GIFI provides the European Commission with the current contact details of authorities authorised to cooperate with the competent authorities of Member States that supervise or control compliance by entities with the provisions on counteracting money laundering and financing of terrorism issued under *Directive 2015/849*.

158. As part of initiating other activities to counteract money laundering and financing of terrorism, the GIFI may also conclude agreements with entities other than obligated institutions, that regard collecting information relevant to the implementation of its tasks. The agreement shall specify the scope and form of providing information and the procedure for its provision.

159. The Financial Security Committee (KBF), providing opinions and advice to the GIFI in the field of counteracting money laundering and financing of terrorism, plays an important

[82] Likewise, a foreign FIU's request to the GIFI should also include identification data as indicated in Article 36(1) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, held by the foreign FIU.

supporting role. The KBF, among others, gives opinions on the national assessment of the risk of money laundering and financing of terrorism and the strategy containing an action plan aimed at mitigating the risk associated with these crimes, issues recommendations and opinions on the application of specific restrictive measures against a person or entity, analyses and assesses legal solutions in the field of counteracting money laundering and financing of terrorism, and presents an opinion on the need to amend the provisions on counteracting money laundering and financing of terrorism. The KBF also issues an opinion on the appropriateness of applying the European Commission's recommendations referred to in Article 6(4) of *Directive 2015/849*.

160. The Committee consists of representatives of the minister competent for the interior, 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 digitisation, the minister – member of the Council of Ministers competent for coordinating the activities of secret services, if appointed by the Prime Minister, the Chairperson of the Polish Financial Supervision Authority, the President of the National Bank of Poland, the Commander in Chief of the Police, the Commander in Chief of the Military Police, the Commander in Chief of the Border Guard, the National Prosecutor, the Head of the Internal Security Agency, the Head of the Central Anti-Corruption Bureau, the Head of the Foreign Intelligence Agency, the Head of the Military Intelligence Service, the Head of the Military Counterintelligence Service, the Head of the National Revenue Administration, and the Head of the National Security Bureau. Due to the scope of the envisaged tasks, the members of the Committee, besides knowledge in the field of counteracting money laundering and financing of terrorism, must also meet the requirements specified in the provisions on the protection of classified information regarding access to "secret" or "top secret" classified information. The Committee is chaired by the General Inspector of Financial Information, while the head of the organisational unit separated in the office supporting the minister competent for public finance in order to ensure the proper implementation of the GIFI's tasks is the vice-chairperson of the Committee.

4.2.2. Obligated Institutions

161. Pursuant to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* obligated institutions include:

(1) domestic 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 that are not 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 Association of Cooperative Savings and Credit Unions within the meaning of the *Act of 5 November 2009 on cooperative savings and credit unions* (Journal of Laws of 2023, item 1278);

(3) domestic payment institutions, domestic electronic money institutions, branches of EU payment institutions, branches of EU and foreign electronic money institutions, small payment institutions, payment service offices and acquirers, within the meaning of the *Act of 19 August 2011 on payment services*;

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

(5) foreign legal persons conducting brokerage activities in the territory of the Republic of Poland, including those conducting such activities 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 this Act;

(6) companies operating a regulated market – in so far as 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 companies, investment fund management companies, AIC managers, branches of management companies and branches of EU managers located in the territory of the Republic of Poland within the meaning of the *Act of 27 May 2004 on investment funds and the management of alternative investment funds*;

(8) insurance companies performing the activities referred to in class I of the Annex to the *Act of 11 September 2015 on insurance and reinsurance activities*, including domestic insurance companies, main branches of foreign insurance companies established in a non-EU country and branches of foreign insurance companies established in an EU Member State other than the Republic of Poland;

(9) insurance brokers performing insurance brokerage activities relating to insurance types listed in class I of the Annex to the *Act of 11 September 2015 on insurance and reinsurance activities*, and branches of foreign intermediaries performing such activities, established in the territory of the Republic of Poland, except for an insurance agent that:

(a) is an insurance agent performing insurance intermediation activities for one insurance company within the same insurance class in accordance with the Annex to the *Act of 11 September 2015 on insurance and reinsurance activities*;

(b) does not charge insurance premiums from the client or the amounts due to the client from the insurance company;

(10) KDPW S.A. and a company commissioned by KDPW S.A. to carry out the activities referred to in Article 48(1)(1) of the *Act of 29 July 2005 on trading in financial instruments*, in so far as they keep securities accounts or omnibus accounts;

(11) currency exchange office operators within the meaning of the *Act of 27 July 2002 – Foreign Exchange Law*, other operators providing currency exchange services or currency exchange intermediation services that are not other obligated institutions, and branches of foreign operators conducting such activities in the territory of the Republic of Poland;

(12) entities conducting business activity consisting in the provision of services in the field of:

(a) exchange between virtual currencies and legal tenders;

(b) exchange between virtual currencies;

(c) intermediation in the exchange referred to in point (a) or (b);

(d) keeping the accounts referred to in Article 2(2)(17)(e) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*;

(13) notaries in so far as they perform activities in the form of a notarial deed, including:

(a) transfer of the ownership of an asset, including sale, exchange or donation of a movable property or real estate;

(b) conclusion of an agreement on the division of inheritance, dissolution of co-ownership, life annuity, pension in exchange for the transfer of the ownership of real estate and on the distribution of jointly held assets;

(c) assignment of the cooperative member's ownership right to premises, perpetual usufruct right, and the alleged promise of separate ownership of premises;

(d) in-kind contribution following a company establishment;

(e) conclusion of an agreement documenting a contribution or an increase in the contributions to a company or a contribution or an increase in the share capital;

(f) transformation or merger of companies;

(g) transfer of an enterprise;

(h) transfer of shares in a company;

(14) notaries with respect to the activities referred to in Article 79(6a) of the *Act of 14 February 1991 – Law on Notaries* (Journal of Laws of 2022, item 1799);

(15) attorneys, legal counsels, foreign lawyers, tax advisors in so far as they provide the client with legal assistance or tax advisory in the area of:

(a) purchase or sale of real estate, an enterprise or an organised part of an enterprise;

(b) management of the client's cash, financial instruments or other assets;

(c) concluding agreements on keeping a bank account, a securities account or performing activities related to keeping these accounts;

(d) in-kind contribution to a capital company or increasing the share capital of a capital company;

(e) establishing, operating or managing capital companies or trusts

- except for legal counsels and foreign lawyers practicing their profession under an employment or service relationship in offices serving public administration bodies, other state or local government organisational units and in entities other than the companies referred to in Article 8(1) of the *Act of 6 July 1982 on legal counsels* (Journal of Laws of 2022, item 1166), and tax advisors practicing their profession under an employment relationship in entities other than those referred to in Article 4(1)(1) and (3) of the *Act of 5 July 1996 on tax advisory services* (Journal of Laws of 2021, item 2117);

(16) tax advisors in so far as they perform tax advisory activities other than those referred to in point 14, and expert auditors;

(17) economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, whose primary activity involves the provision of services consisting in

drawing up declarations, keeping tax books, providing advice, opinions or explanations regarding tax or customs legal provisions, that are not other obligated institutions;

(18) economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, that are not other obligated institutions, providing services consisting in:

(a) acting as a formation agent of a legal person or an organisational unit without legal personality;

(b) acting as a member of the management board or arranging for another person to perform this function or a similar function in a legal person or an organisational unit without legal personality;

(c) providing a registered office, business address or correspondence address and other related services to a legal person or an organisational unit without legal personality;

(d) acting or arranging for another person to act as the trustee of a trust established by means of a legal act;

(e) acting or arranging for another person to act as a nominee shareholder for an entity other than a company listed on a regulated market subject to disclosure requirements under the European Union law or subject to equivalent international standards;

(19) entities conducting business consisting in the provision of bookkeeping services;

(20) real estate brokers within the meaning of the *Act of 21 August 1997 on real estate management*, except for real estate intermediation activities aimed at concluding an ordinary or usufructuary lease agreement for real estate or part thereof, with a monthly rent in an amount lower than the equivalent of EUR 10,000;

(21) postal operators within the meaning of the *Act of 23 November 2012 – Postal Law*;

(22) entities conducting business in the field of games of chance, betting, card games and games on gaming machines within the meaning of the *Act of 19 November 2009 on gambling*;

(23) foundations established pursuant to the *Act of 6 April 1984 on foundations*, in so far as they accept or make cash payments in an amount equal to or greater than the equivalent of EUR 10,000, regardless of whether the payment is carried out as a single operation or several operations that appear to be related to each other;

(24) associations with legal personality, established pursuant to the *Act of 7 April 1989 – Law on Associations*, in so far as they accept or make cash payments in an amount equal to or greater than the equivalent of EUR 10,000, regardless of whether the payment is carried out as a single operation or several operations that appear to be related to each other;

(25) economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, in so far as they accept or make cash payments for goods in an amount equal to or greater than the equivalent of EUR 10,000, regardless of whether the payment is carried out as a single operation or several operations that appear to be related to each other;

(26) economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, in so far as they conduct activity consisting in making safe deposit boxes

available, as well as branches of foreign economic operators conducting such activity in the territory of the Republic of Poland;

(27) economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, conducting business consisting in:

(a) trade in or intermediation in the trade in works of art, collectibles and antiques within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services*, also where such activity is carried out:

- in art galleries or auction houses or
- using a free port, understood as a zone or room where goods are treated as not located within the customs territories of Member States or third countries, also with the use of a duty-free zone;

(b) storage of works of art, collectibles and antiques within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services*, where such activity is carried out using a free port referred to in point (a) second indent

- with respect to transactions with a value equal to or greater than the equivalent of EUR 10,000, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other;

(28) lending institutions within the meaning of the *Act of 12 May 2011 on consumer loans*.

162. Pursuant to the Act obligated institutions are required to apply customer due diligence measures. The extent of customer due diligence measures accounts for the identified risk of money laundering and financing of terrorist related to business relationships or an occasional transaction, as well as its assessment. Obligated institutions are also required to document the identified risk and apply customer due diligence measures to the extent and with intensity accounting for the identified risk. At the request of the authorities indicated in the Act, including the GIFI, obligated institutions shall demonstrate that, having regard to the level of the identified risk of money laundering and financing of terrorism related to given business relationships or occasional transaction, they have applied adequate customer due diligence measures. The burden of proving the adequate application of customer due diligence measures rests with the obligated institution. In accordance with the risk-based approach, it is the obligated institution that ultimately decides to what extent and with what intensity it will apply customer due diligence measures in a given case. This institution must also demonstrate the adequate selection of these measures.

163. Obligated institutions apply customer due diligence measures in the case of:

(1) establishing business relationships;

(2) carrying out an occasional transaction with a value equivalent to EUR 15,000 or more, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other, or which constitutes a transfer of funds in an amount exceeding the equivalent of EUR 1,000; in the case of obligated institutions that are entities conducting business activity consisting in providing services in the field of exchange between virtual currencies and legal tenders, exchange between virtual currencies, intermediation in the exchange referred to above, keeping accounts

– in electronic form – a set of identification data ensuring that authorised persons can use virtual currency units to, among others, exchange them using a virtual currency equivalent to EUR 1,000 or more;

(3) carrying out an occasional cash transaction with a value equivalent to EUR 10,000 or more, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other, in the case of obligated institutions being foundations established pursuant to the *Act of 6 April 1984 on foundations*, associations with legal personality established pursuant to the *Act of 7 April 1989 – Law on Associations*, operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, that accept or make cash payments for goods in an amount equal to or greater than the equivalent of EUR 10,000;

(4) putting stakes and collecting winnings equivalent to EUR 2,000 or more, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other – in the case of the aforementioned entities conducting business activity in the field of games of chance, betting, card games and games on gaming machines;

(5) suspicion of money laundering or financing of terrorism;

(6) doubts as to the veracity or completeness of the customer's identification data obtained so far.

164. Obligated institutions may apply simplified customer due diligence measures in cases where the risk assessment has confirmed the existence of a lower risk of money laundering or financing of terrorism. The obligated institution shall, however, apply enhanced customer due diligence measures in cases of business relationships or occasional transactions associated with a higher risk of money laundering or financing of terrorism, as well as, among others, with respect to customers coming from or based in a high-risk third country.

165. In order to mitigate the risk of money laundering and financing of terrorism and properly manage the identified risk of money laundering or financing of terrorism, obligated institutions are required to introduce an internal procedure for counteracting money laundering and financing of terrorism and to designate a person holding a managerial position to be responsible for the fulfilment of the obligations specified in the Act.

166. Obligated institutions are also required to develop and implement an internal procedure for anonymous reporting by employees or other persons performing activities for the obligated institution of actual or potential violations of the provisions on counteracting money laundering and financing of terrorism.

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

(1) The following transactions carried out by all obligated institutions, with the exception of currency exchange office operators, other operators providing currency exchange services or currency exchange intermediation services (that are not other obligated institutions), branches of foreign economic operators conducting such activities in the territory of the Republic of Poland, notaries, attorneys, legal counsels, foreign lawyers and tax advisors, expert auditors, economic operators whose primary activity involves

the provision of services consisting in drawing up declarations, keeping tax books, providing advice, opinions or explanations regarding tax or customs legal provisions, that are not other obligated institutions, real estate brokers:

(a) accepted payment or executed disbursement of cash equivalent to more than EUR 15,000;

(b) executed transfer of funds[83] equivalent to more than EUR 15,000 (also in the case of a transfer originating from outside the Republic of Poland to a recipient for whom the obligated institution acts as payment service provider), with certain exceptions specified in its provisions;

(2) An executed foreign currency purchase or sale transaction equivalent to more than EUR 15,000, or intermediation in such transaction, by all obligated institutions;

(3) Notarial acts with a value equivalent to more than EUR 15,000, performed by notaries (but only as regards notarial acts in the case of which they are obligated institutions).

168. Obligated institutions are also required to notify the GIFI of circumstances that may indicate a suspicion of committing a money laundering or terrorism financing offence, with no delay, but no later than within 2 business days from the date of confirming these circumstances.

169. They are also required to notify the GIFI with no delay of cases of becoming aware of a reasonable suspicion that a specific transaction or specific assets may be associated with money laundering or financing of terrorism. In this case, until the obligated institution receives a request to block the account or suspend the transaction or until it has not been released from this obligation, but no longer than for 24 hours from the moment of confirming receipt of the notification, it shall not carry out the transaction with respect to which there is a reasonable suspicion that it may be related to money laundering or financing of terrorism or other transactions debiting the account with suspicious assets that may be related to money laundering or financing of terrorism.

170. At the request of the GIFI (issued both as a result of a notification submitted by an obligated institution and irrespectively of such notification), obligated institutions shall block accounts or suspend transactions for the period indicated in the request. If the request to suspend a transaction or block an account submitted by the GIFI to the obligated institution results from the obligated institution's notification of becoming aware of a reasonable suspicion that the transaction or assets may be related to money laundering or financing of terrorism, the account blockade or transaction suspension imposed by the GIFI shall last no longer than 96 hours from the date and time indicated in the confirmation of the notification receipt. In other situations, the account blockade or transaction suspension imposed by the GIFI shall last no longer than 96 hours from the request receipt by the obligated institution.

[83] Within the meaning 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 (OJ L 141, 05.06.2015, p. 1), i.e. relating to transactions carried out through payment service providers.

171. Obligated institutions (except for domestic banks, branches of foreign banks, branches of credit institutions[84] and cooperative savings and credit unions[85]) shall block accounts or suspend transactions for no longer than 96 hours from the moment of submitting to the competent prosecutor a notification of becoming aware of a reasonable suspicion that the assets being the subject of the transaction or deposited in the account originate from an offence other than money laundering or financing of terrorism or a fiscal offence or are related to an offence other than money laundering or financing of terrorism or a fiscal offence. If the prosecutor issues a decision to initiate proceedings, they shall suspend the transaction or block the account by way of a decision for no longer than 6 months from the date of the notification receipt.

172. The GIFI may exempt the obligated institution from the requirement to refrain from carrying out a transaction reported in the manner described above if the information held does not provide grounds for notifying the prosecutor of a suspicion of committing a money laundering or terrorism financing offence, or if it is considered that suspending the transaction or blocking the account could hinder performing their tasks by judicial authorities and services or institutions responsible for protecting public order, security of citizens or prosecuting perpetrators of offences or fiscal offences.

173. At the request of the GIFI, obligated institutions shall transfer or make available, with no delay, information or documents they hold, necessary for the implementation of its tasks, including those relating to: their customers, transactions carried out – as regards the data specified in the Act (Article 72(6), among others, unique transaction identifier, the date and time of the transaction, identification data of the customer issuing the order, identification data of the other parties, the amount and currency of the transaction), the type and amount of the assets and the location of their storage, application of a customer due diligence measure – ongoing monitoring of the customer's business relationships, IP addresses from which connections to the ICT system of the obligated institution were made and duration of such connections.

174. The GIFI may also request the obligated institution to monitor indicated business relationships or occasional transactions. The GIFI shall specify in its request the scope of information obtained through monitoring and the time of its obtaining (i.e. monitoring time), as well as the date and form of transferring or making available the information or documents to the GIFI.

---

[84] Banks – if they become aware of a reasonable suspicion that the funds deposited in a bank account originate from or are related to, in whole or in part, a fiscal offence or an offence other than an offence under Article 165a or Article 299 of the Penal Code – are authorised to block the funds in this account for no longer than 72 hours (pursuant to Article 106a(3) of the *Act of 29 August 1997 – Banking Law*). If the prosecutor issues a decision to initiate proceedings (having received a relevant notification from the bank), they may, by way of a decision, suspend a specific transaction or block the funds in the account for no longer than 6 months from the date of receipt of the notification.

[85] Cooperative savings and credit unions – if they become aware of a reasonable suspicion that the funds deposited in an account originate from, in whole or in part, a fiscal offence or an offence other than an offence under Article 165a or Article 299 of the Penal Code – are authorised to block the funds in this account for no longer than 72 hours (pursuant to Article 16(3) of the *Act of 5 November 2009 on cooperative savings and credit unions*). If the prosecutor issues a decision to initiate proceedings (having received a relevant notification from the cooperative savings and credit union), they may, by way of a decision, suspend a specific transaction or block the funds in the account for a specified period, no longer than 6 months from the date of receipt of the notification.

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

176. The GIFI controls whether obligated institutions fulfil their obligations in the field of counteracting money laundering and financing of terrorism. Control over obligated institutions is exercised also, within the scope of their powers, by the following authorities in accordance with the rules laid down in other provisions:

- President of the National Bank of Poland (with respect to currency exchange office operators within the meaning of the *Act of 27 July 2002 – Foreign Exchange Law*),
- Polish Financial Supervision Authority (with respect to obligated institutions supervised by it),
- National Association of Cooperative Savings and Credit Unions (with respect to cooperative savings and credit unions),
- presidents of courts of appeal (with respect to notaries),
- heads of customs and tax control offices (with respect to obligated institutions controlled by these authorities).

177. Such control may be carried out on the terms set out in the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* also by voivodeship or poviat governors – with respect to associations, and by ministers or poviat governors – with respect to foundations.

An obligated institution that violates the obligations laid down in the Act and in the *provisions of Regulations 2015/847*[86]*, 881/2002*[87]*, 753/2011*[88] and *2580/2001*[89] shall be subject to an administrative sanction.

178. Pursuant to the Act, administrative sanctions include:

- publication of information about the obligated institution and the scope of the violation of the provisions of the Act by this institution in the Public Information

[86] 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 141, p. 1, as amended).
[87] Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan (OJ L 139, p. 9, as amended).
[88] Council Regulation (EU) No 753/2011 of 1 August 2011 concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan (OJ L 199, p. 1, as amended).
[89] Council Regulation (EC) No 2580/2011 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (OJ L 344, p. 70, as amended).

Bulletin, on the website of the office supporting the minister competent for public finance,

- ordering the obligated institution to discontinue specific activities,
- revoking the licence or permit or removal from the register of regulated activities,
- ban on performing duties in a managerial position by the person liable for the violation of the provisions of the Act by the obligated institution, for a maximum period of one year,
- fine.

4.2.3. Cooperating units

179. Pursuant to the Act, cooperating units include government administration bodies, local government bodies and other state organisational units, as well as the National Bank of Poland, the Polish Financial Supervision Authority and the Supreme Audit Office.

180. At the request of the GIFI, cooperating units provide or make available, within their statutory powers, information and documents held. In order to provide or make available the aforementioned information or documents, the GIFI may conclude an agreement with a cooperating unit, specifying the technical conditions for providing or making available information or documents.

181. Cooperating units shall also notify the GIFI with no delay of a suspicion of committing a money laundering or terrorism financing offence and develop instructions on how to proceed in such cases. If based on the aforementioned notifications, the GIFI notified the prosecutor's office of a suspicion of committing one of the aforementioned offences, the GIFI shall communicate this fact – within 30 days from the date of submitting the notification to the competent prosecutor – to the cooperating unit that provided the information on which the notification was based. The GIFI, no later than within 30 days, shall notify the Internal Security Agency, the Central Anti-Corruption Bureau, the Police, the Military Police and the Border Guard of circumstances indicating a connection between the information contained in notifications on a suspicion of committing a money laundering or terrorism financing offence provided by cooperating units and the information received from obligated institutions, regarding:

- circumstances that may indicate a suspicion of committing a money laundering or terrorism financing offence,
- cases of becoming aware of a reasonable suspicion that a specific transaction or specific assets may be related to money laundering or financing of terrorism,
- notifying the competent prosecutor of becoming aware of a reasonable suspicion that the assets being the subject of a transaction or deposited in an account originate from an offence other than money laundering or financing of terrorism or from a fiscal offence, or are related to an offence other than money laundering or financing of terrorism or with a fiscal offence.

182. The Border Guard bodies and the heads of customs and tax control offices used to provide the GIFI with the information referred to in Article 5 of *Regulation (EC) No 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 information contained in the notification specified in the regulations issued pursuant to Article 21 of the *Act of 27 July 2002 – Foreign Exchange Law*. This information was provided by the 14th day of the month following the month in which cash entered or left the territory of the Republic of Poland. The heads of customs and tax control offices and the Border Guards bodies provided information through the Head of the National Revenue Administration and the Commander in Chief of the Border Guard, respectively. Currently, according to the information contained in the GIFI's report for 2021: "Due to the entry into force of a regulation[90] at the European Union level, from June 2021, the provisions of Article 85(1) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, under which bodies of the Border Guard and the National Revenue Administration provided to the GIFI information from declarations on cash transport across the EU border, became irrelevant. Since June 2021, data from these declarations has been entered directly in the pan-European Customs Information System (CIS) to which the GIFI has gained access. Following this change, information on declarations is no longer reported to the GIFI, and the GIFI has access to it via the aforementioned European system".

183. Moreover, the GIFI provides the information it holds upon a written and substantiated request of:

(1) Commander in Chief of the Police;

(2) Commander of the Central Investigation Bureau of the Police,

(3) Commander in Chief of the Military Police;

(4) Commander in Chief of the Border Guard;

(5) Head of the Internal Security Agency;

(6) Head of the Foreign 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 Internal Affairs Bureau of the Police;

(12) Commander of the Internal Affairs Bureau of the Border Guard;

(13) Commander of the Central Office for Combating Cybercrime

– or persons authorised by them, within the scope of their statutory tasks.

184. The GIFI provides the information it holds also upon a written and substantiated request of:

[90] *Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (OJ L 284, 12.11.2018).*

- Chairperson of the Polish Financial Supervision Authority – as regards supervision exercised by the Polish Financial Supervision Authority pursuant to the *Act of 21 July 2006 on financial market supervision*,
- President of the National Bank of Poland – in so far as necessary to carry out control proceedings specified in the *Act of 27 July 2002 – Foreign Exchange Law*, with respect to operators carrying out currency exchange activity within the meaning of this Act,
- President of the National Bank of Poland – in so far as necessary to carry out control proceedings specified in the *Act of 23 December 1994 on the Supreme Audit Office*,
- 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, 3.05.2013) – within the scope of its powers,
- minister competent for foreign affairs – within the scope of its statutory powers in connection with the application of specific restrictive measures,
- minister competent for public finance – in connection with the request referred to in Article 11(2) of the *Act of 19 November 2009 on gambling*.

185. The GIFI provides the information it holds upon a written and substantiated request of the Head of the National Revenue Administration, the director of a regional revenue administration office or the head of a customs and tax control office, within the scope of their statutory tasks.

186. In particularly justified cases, the GIFI may refuse to make the information held available to the aforementioned entities, where its disclosure:

- will negatively affect the process of analysing by the GIFI information on assets suspected to be related to a money laundering or terrorism financing offence,
- exposes a natural or legal person or an organisational unit without legal personality to disproportionate damage,
- is irrelevant for the purposes referred to in the request.

187. Where it is suspected that a fiscal offence or an offence other than money laundering or financing of terrorism has been committed, the GIFI shall provide information substantiating this suspicion to the competent authorities (i.e. the aforementioned law enforcement agencies, secret services or the Head of the KAS), so that they can take steps as part of their statutory tasks. The GIFI may also make the information held available to the aforementioned authorities *ex officio*, so that they can take steps as part of their statutory tasks. Furthermore, in the event of a reasonable suspicion of a violation of regulations related to the operation of the financial market, the GIFI shall provide the information substantiating this suspicion to the Polish Financial Supervision Authority. In the above situations, cooperating units shall send feedback on how they have used the received information within 90 days from the date of its receipt.

188. The Act obliges prosecutors to notify the GIFI of issuing a decision on:

- blocking an account or suspending a transaction,
- initiating proceedings,
- bringing an accusation,
- bringing an indictment

in cases involving money laundering or financing of terrorism. The aforementioned information is transferred with no delay, but no later than within 7 days from the date of the action. The information should indicate, in particular, the circumstances of committing the offence, along with the available identification details of natural persons, legal persons or organisational units without legal personality, and the file reference number. The Act also provides for an information obligation imposed on the GIFI. Namely, having received information from the prosecutor about the issued decisions, the GIFI is obliged to inform the prosecutor without delay about being in possession of information related to the information received from the prosecutor. It should be emphasised that the GIFI's obligation is limited only to notifying about being in possession of information, and not to transmitting it. The prosecutor, within their powers, may apply to the GIFI to obtain this information.

189. A statutory obligation has also been imposed on prosecutors to notify the GIFI, within 30 days (after having been informed by the GIFI about the suspicion of committing the offence referred to in Article 299 or 165a of the Penal Code), of:

- issuing a decision to block a bank account or suspend a transaction,
- suspending proceedings,
- resuming suspended proceedings,
- issuing a decision to bring charges.

190. The regulation concerned is supplementary to the criminal procedure provisions regarding the prosecutor's obligations as regards the response to the submitted notification. The rationale for the government's draft *Act on counteracting money laundering and financing of terrorism* (pp. 53-54) reads: "Obtaining feedback by the General Inspector of Financial Information is an important factor ensuring the required effectiveness of analytical proceedings conducted by the General Inspector."

4.3. PERSONAL DATA PROTECTION

191. Provisions limiting the disclosure of confidential information or data, with the exception of classified information within the meaning of the provisions on the protection of classified information, shall not apply to 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*.

192. In carrying out its tasks, the GIFI may collect and use the necessary information containing personal data and process it within the meaning of the provisions on the protection of personal data (also without the knowledge and consent of the data subject), create personal data sets, 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

2022, item 1648), i.e. information regarding IP addresses from which the connection to the IT system of the obligated institution was made and the 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 preventing and combating crime* (Journal of Laws of 2023, item 1206)[91], i.e. sensitive data such as personal data revealing racial and ethnic origin, political opinions, religious and philosophical beliefs, membership in trade unions, processing of genetic and biometric data in order to clearly identify a natural person, data regarding health, sexuality and sexual orientation of a natural person, the GIFI shall collect, store and process this data only where it is actually necessary due to the scope of tasks or activities performed.

193. The GIFI shall process financial information, including personal data, for the period during which this information is necessary for it to perform its statutory tasks. At least once every 5 years, the GIFI shall verify the need for the further processing of the collected information. Information that is not necessary for the implementation of the statutory tasks is immediately deleted by the Commission appointed by the GIFI.

194. The GIFI shall provide, only at the request of a court or prosecutor, where necessary for pending proceedings, personal data of:

(1) natural persons submitting – on behalf of obligated institutions – notifications of:

(a) circumstances that may indicate a suspicion of committing a money laundering or terrorism financing offence, or

(b) in cases of a reasonable suspicion that a specific transaction or specific assets may be related to money laundering or financing of terrorism;

(2) persons reporting suspicions of money laundering or financing of terrorism within the internal structures of obligated institutions;

(3) persons reporting violations of provisions relating to counteracting money laundering and financing of terrorism;

(4) employees of the Department of Financial Information dealing with:

(a) analysing information concerning assets suspected by the GIFI of being related to a money laundering or terrorism financing offence;

(b) suspending transactions or blocking banks accounts;

(c) requesting information on transactions and making it available;

(d) providing authorised authorities with information and documents substantiating a suspicion of committing an offence;

(e) sharing information with cooperating units.

195. The procedure for making information held by the GIFI available to courts, law enforcement authorities, secret services, the head of the National Revenue Administration, the President of the National Bank of Poland, the Office of the Polish Financial Supervision

[91] Introducing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, directly applicable in all EU countries, did not automatically repeal the aforementioned provision.

Authority, the President of the Supreme Audit Office, and foreign financial intelligence units is provided for in Articles 103, 104, 105, 106 and Articles 110-116 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. The GIFI may also exchange information related to money laundering or financing of terrorism with the European Union Agency for Law Enforcement Cooperation (EUROPOL), either directly or through the EUROPOL National Unit. Moreover, the GIFI may share and obtain information as part of cooperation with competent authorities of other countries, foreign institutions, and international organisations dealing with counteracting money laundering or financing of terrorism, as well as EU supervisory authorities. In order to pursue this cooperation, the General Inspector may conclude agreements specifying the procedure and technical conditions for providing or obtaining information.

196. Personal data provided to a prosecutor or court may not be made available to other entities or persons, except for the persons referred to in:

- Article 156(1) of the *Code of Criminal Procedure*, i.e.: in the course of court proceedings – to the parties, defence attorneys, attorneys and statutory representatives, as well as to other persons with the consent of the president of the court (it is also possible to make transcripts or copies of case files), also via the IT 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, "where it is not necessary to ensure the proper course of the proceedings or protect an important interest of the state" – to the parties, defence attorneys, attorneys and statutory representatives, and also in exceptional cases, with the consent of the prosecutor, to other persons (enabling the preparation of transcripts or copies of case files and issuing, against payment, certified transcripts or copies), also in electronic form;
- Article 321(1) of the *Code of Criminal Procedure* (in the course of an investigation, if there are grounds for closing this investigation – to the suspect or their defence attorney at their request, also in electronic form).

197. All information collected and made available by financial information authorities in accordance with the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* shall be covered by financial information secrecy. The GIFI shall make it available only under 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 Department of Financial Information of the Ministry of Finance, as well as persons performing activities for this unit otherwise than under an employment relationship are obliged to keep financial information confidential. This obligation prevails also after the termination of the financial information authority function, employment in the aforementioned unit or performing activities for it otherwise than under an employment relationship.

198. The aforementioned obligation to maintain the secrecy of financial information applies also to persons acting as bodies authorised to obtain information in the manner provided for in the Act as well as employees, officers and persons performing activities on their behalf.

However, these bodies as well as employees and officers performing activities on their behalf may exchange information on providing or obtaining information in the manner provided for in the Act, where this is necessary to ensure the accuracy of the tasks performed by them.

199. Persons acting as bodies authorised to obtain information in the manner provided for in the Act as well as employees, officers and persons performing activities on their behalf shall provide information covered by financial secrecy if they are required to do so under other regulations.

200. Information collected and made available by financial information authorities, subject to secrecy obligations specified in other regulations, shall be made available to the extent and under the terms specified in these regulations.

201. In 2018, a 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 natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (OJ L 119, 4.5.2016, p. 1).

202. Separate control as regards obtaining information covered by telecommunications secrecy by the GIFI is exercised by the Regional Court in Warsaw.

4.4. Central Register of Beneficial Owners

203. The Central Register of Beneficial Owners (CRBO) was established pursuant to Article 194 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* as a result of implementing the provisions of *Directive 2015/849* and *Directive 2018/843* into the Polish legal system. The purpose of the CRBO is to provide accurate and valid data on beneficial owners, which is crucial for combating money laundering and financing of terrorism, as it prevents criminals from hiding their identity in a complex corporate structure. The CRBO has been designed to process information on beneficial owners, which pursuant to Article 2(2)(16) of the aforementioned Act includes, in particular, its obtaining, collecting, recording, storing, developing, altering, making available and deleting. The minister competent for public finance shall be the authority competent for the CRBO.

204. The CRBO is maintained using an IT system. The CRBO is public. The provisions of Article 15(1)(c) of *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (OJ L 119, 4.5.2016, p. 1, as amended), hereinafter referred to as GDPR, shall not apply to the processing of personal data collected in the CRBO.

205. The tasks of the authority competent for the CRBO shall include:

- maintaining the Register and determining the organisational and technical conditions on which it is maintained,
- processing information on beneficial owners and information on persons statutorily authorised to represent the entity obliged to report and update information on beneficial owners,

- developing statistical analyses of information processed in the Register,
- imposing, by way of a decision, fines on entities that have failed to fulfil the obligation to report or update information required to be reported to the CRBO, and on beneficiaries who have failed to fulfil the obligation to provide the aforementioned entities with information and documents necessary to report information on the beneficiary to the CRBR and update this information in the CRBO,
- taking steps to ensure that the information contained in the Register is accurate and valid.

206. The authority competent for the CRBO is responsible, among others, for carrying out statistical analyses regarding information processed in the CRBO as required in Article 44 of *Directive 2015/849*, pursuant to which Member States shall ensure that they are able to review the effectiveness of their systems for counteracting money laundering or financing of terrorism by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems, in order to enable providing feedback and an ongoing review of the effectiveness of their systems for counteracting money laundering and financing of terrorism. The authority competent for the Register is authorised to impose fines on a beneficial owner who has failed to fulfil the obligation to provide relevant information to an entity obliged to make an entry in the CRBO. Imposing obligations on beneficial owners towards obligated entities enables these entities to effectively enforce the provision of information by beneficial owners, which in turn aims to ensure the adequacy, accuracy and validity of data processed in the CRBO.

207. The obligation to report and update information on beneficial owners applies to:

(1) general partnerships;

(2) limited partnerships;

(3) limited joint-stock partnerships;

(4) limited liability companies;

(5) simple joint-stock companies;

(6) joint-stock companies, except for public companies within the meaning of the *Act of 29 July 2005 on public offering and conditions for introducing financial instruments to an organised trading system and on public companies* (Journal of Laws of 2022, item 2554);

(7) trusts whose trustees or persons holding equivalent positions:

(a) reside or are established in the territory of the Republic of Poland, or

(b) establish business relationships or acquire real estate in the territory of the Republic of Poland on behalf of or for a trust;

(8) partnerships;

(9) European Economic Interest Groupings;

(10) European companies;

(11) cooperatives;

(12) European cooperatives;

(13) associations subject to an entry in the National Court Register (KRS);

(14) foundations;

(15) family foundations.

208. The scope of information subject to reporting is specified in Article 59 of the Act.

209. The obligated institution shall record discrepancies between the information collected in the Register and the information regarding the customer's beneficial owner it has determined, takes steps to explain the reasons for these discrepancies, and if the recorded discrepancies have been confirmed, the obligated institution shall provide the authority competent for the Register with verified information on these discrepancies. The authority competent for the Register may initiate proceedings to clarify whether the information collected in the Register is accurate and valid.

210. Cooperating units may also notify recorded discrepancies between the information collected in the Register and the information regarding beneficial owners they have, and where discrepancies are recorded, the cooperating entity shall provide the authority competent for the Register with verified information regarding these discrepancies.

211. Having obtained information regarding recorded discrepancies, the authority competent for the Register shall take steps to clarify them.

4.5. Register of trust and company service providers and the register of virtual currency service providers

212. At the end of October 2021, provisions amending the *Act on counteracting money laundering and financing of terrorism*, regarding the establishment of legal requirements for conducting business in the field of virtual currencies, entered into force. This activity gained the status of a regulated activity that may be conducted only following its prior registration. The foregoing applies also to services provided for companies or trusts, that have also become a regulated activity.

213. The matters related to the register of trust and company service providers and the register of virtual currency service providers fall within the competence of the minister competent for public finance.

214. According to the information posted on the website of the Regional Revenue Administration Office in Katowice[92], as at 19 May 2023, the register of trust and company service providers included 1,878 entities.

215. Entry in the register is obligatory for trust and company service providers that carry the following activities:

- acting as a formation agent of a legal person or an organisational unit without legal personality,

[92]https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestrdzialalnosci-na-rzecz-spolek-lub-trustow

- acting as a member of the management board or arranging for another person to perform this function or a similar function in a legal person or an organisational unit without legal personality,
- providing a registered office, business address or correspondence address and other related services to a legal person or an organisational unit without legal personality,
- acting or arranging for another person to act as trustee of a trust that has been established by legal action,
- acting or arranging for another person to act as a nominee shareholder for an entity other than a company listed on a regulated market subject to disclosure requirements under European Union law or subject to equivalent international standards.

216. As far as entities subject to obligatory entry in the register of virtual currency service providers are concerned, these are entities conducting business consisting in the provision of services in the field of:

- exchange between virtual currencies and legal tenders,
- exchange between virtual currencies,
- intermediation in the aforementioned exchange,
- maintaining accounts, i.e. sets of identification data kept in electronic form, enabling authorised persons use virtual currency units, including carrying out their exchange transactions.

217. In reference to the above, it should be noted that obligatory entry in the register of virtual currency service providers applies to four groups of entities:

- economic operators dealing in the exchange of legal tenders (e.g. Polish zloty, dollar, euro) for virtual currencies (e.g. Bitcoin, Ethereum) or vice versa,
- entities that exchange virtual currencies (e.g. Bitcoin, Ethereum),
- intermediaries in the exchange between virtual currencies or legal tenders and virtual currencies,
- entities maintaining special accounts where virtual currencies are deposited, used, in particular, for conducting transactions aimed at exchanging virtual currencies.

218. It should be emphasised that it does not matter whether any of the above activities are performed by a natural person, a legal person or a legal entity with limited legal capacity (e.g. a commercial partnership) – all of them should be entered in the register.

219. The relatively simple method of registration (applications are submitted via an electronic inbox) does not affect in any way the general legal requirements to be met by economic operators dealing with virtual currencies. First of all, the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* introduces the requirement of having no criminal record for specific offences and intentional fiscal offenses (this applies, among others, to members of the management bodies and beneficial owners of the applicant) and having relevant knowledge or experience in running a virtual currency business (the requirement is considered to be met upon completion of a course on the legal and practical

aspects of cryptocurrency business). The requirement of having no criminal record and having relevant knowledge applies similarly to trust or company service providers.

220. Such economic operators also have the status of an obligated institution under the provisions of the Act, which means that they have to apply customer due diligence measures (e.g. identification and verification of customers' identity) and implement an internal policy for counteracting money laundering and financing of terrorism.

221. Running business activity without the relevant entry in the register may result in a fine of up to PLN 100,000 (a similar regulation applies to both registers, so it applies to trust or company service providers and virtual currency service providers).

222. It should be noted that the mere registration of a business does not necessarily ensure full compliance with regulatory requirements. It may be necessary, for example, to apply for other authorisations to conduct business on the financial market (e.g. in the case of the provision of payment services). Meeting the registration obligation will be sufficient only where the conducted activity does not overlap with other regulated activities that may require a separate entry or even a permit.

223. New regulations providing for the obligation to register business activity in the field of virtual currencies should be considered an evolution in the regulation of the financial market in the part relating to the crypto-assets sector. However, attention should be paid to emerging doubts regarding the scope of the regulation that does not cover directly all service providers dealing with trading in cryptocurrencies, including their issuers.

224. At the EU level, work was carried out in 2022 on the *Regulation on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937* (MiCA). Following the adoption of this Regulation by the European Parliament and the Council on 31 May 2023, the Regulation was published on 9 June 2023 in the Official Journal of the EU L.2023.150.40. Therefore, Polish regulations – due to the adopted EU Regulation – must be adapted to its wording in the near future. The Regulation entered into force on the twentieth day following its publication in the Official Journal of the European Union, but its provisions will apply (in principle) after 18 months from the date of its entry into force.

The MiCA Regulation was proposed by the European Commission on 24 September 2020. It is part of a broader digital finance package that is intended to foster technological development at the EU level while ensuring financial stability and consumer protection. Besides the MiCA proposal, the package also includes a digital finance strategy, a proposal for a Digital Operational Resilience Act (DORA) – that covers also crypto-asset service providers – and a proposal for a pilot regime for market infrastructures based on distributed ledger technology (DLT). This package aims to fill a gap in EU regulations: ensure that the existing legal framework does not hinder the use of new digital financial instruments, while ensuring that such new technologies and products are covered by financial regulations and operational risk management solutions for companies operating in the EU. The package is therefore intended to foster innovation and the dissemination of new financial technologies, while ensuring adequate protection for consumers and investors. The Council adopted its negotiating mandate on MiCA on 24 November 2021. The trilogue between the co-legislators started on 31 March 2022 and ended on 30 June 2022 with a provisional agreement.

225. To the extent not regulated otherwise, the provisions of the *Act of 6 March 2018 – Economic Operators' Law* shall apply to the registers.

226. The purpose of the regulation is to impose the obligation to obtain entry in the register on those economic operators whose services generate the risk of money laundering or financing of terrorism. According to the recitals of *Directive 2018/843*, providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers are under no Union obligation to identify suspicious activity, as a result of which terrorist groups may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity. The requirement introduced by Polish regulations to consider economic operators engaged in currency exchange services obligated institutions (as a result of which these entities are obliged to apply customer due diligence measures) was also due to the findings made by the FATF (e.g. Terrorist Financing Disruption Strategies, 2018) that confirm that virtual currencies are used by terrorist groups as one of the main mechanisms to transfer funds. The purpose of obtaining entry into the register of virtual currency service providers is also to increase the transparency of transactions on the financial market.

5. THREATS RELATED TO MONEY LAUNDERING

5.1. THREATS RELATED TO PREDICATE OFFENCES

227. Money laundering is penalised under Article 299 of the *Penal Code* where the nature of this illegal practice is defined. An offence specified in that article may cover assets derived directly or indirectly from a prohibited act, and the perpetrator of a predicate offence from which the laundered money originates may also be considered the perpetrator of money laundering. Article 299 of the *Penal Code*, penalising money laundering, indicates that this practice may cover "legal tenders, financial instruments, securities, foreign exchange values, property rights or other movable or immovable property derived from benefits related to committing 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. acts prohibited by law under the pain of a penalty. According to data of the Ministry of Justice, in 2022, 316 (300 in 2021) criminal court proceedings regarding the offence under Article 299 of the *Penal Code* were instituted in 2022 against 823 (997 in 2021) persons by district and regional courts in Poland. During the same period, the courts concluded 261 (226 in 2021) criminal proceedings in cases regarding the aforementioned offence. According to data of the Ministry of Justice, in 2022, 236 (295 in 2021) persons were finally sentenced for committing the offence of money laundering under Article 299 of the *Penal Code*, while 547 (426 in 2021) persons were sentenced for committing this offence in the first instance. In the proceedings conducted in 2022, property for the total amount of PLN 2,883,999 (PLN 10,380,390 in 2021) was secured, assets in the amount of PLN 397,000 (PLN 1,554,377 in 2021) were seized, and the forfeiture of property for the total amount of PLN 213,043,034 (PLN 170,720,814 in 2021) was ordered.

228. Therefore, any type of offence as a result of which the perpetrator generates proceeds may be considered a predicate offence for money laundering. Predicate offences may include corruption offences, offences committed on the financial market (including stock exchange offences, insurance offences, conducting business without a licence), fiscal offences, trafficking in narcotic drugs and psychotropic substances, human trafficking and migrant smuggling, illegal gambling, offences related to the infringement of copyright and industrial property rights, offences against property and against economic transactions as well as other offences[93].

Table 5. Offences ascertained[94] by the Police and the Public Prosecutor's Office in completed

[93] In this respect, it is worth indicating that the offence specified in Article 165a of the Penal Code is also a predicate offence for money laundering. This is compliant with FATF Recommendation 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).

[94] An ascertained offence is an incident that has been confirmed as a criminal offence in concluded preparatory proceedings. The data does not include criminal acts committed by minors.

preparatory proceedings in 2020-2021 (extract from the GUS statistical yearbooks for 2021 and 2022)[95]

Type of offence	Number	
	2020	2021
Total of which:	774,974	829,102
offences against property	370,836	418,643
offences against general security and traffic security	72,958	77,853
offences against document credibility	50,302	53,577
offences against family and care	57,897	56,804
offences against the activities of state institutions and local government institutions	27,486	28,873
offences against freedom, freedom of conscience and religion	27,945	27,977
offences against life and health	15,835	15,004
offences against justice	20,128	23,716
offences against economic transactions	5,532	5,746
offences against money and securities trading	5,078	5,204
offences against public order	5,490	6,298
offences against sexual freedom and morality	8,819	8,029
offences against honour and physical integrity	3,824	3,917
offences under specific laws:		
on counteracting drug addiction – the Act of 24 April 1997 (consolidated text: Journal of Laws of 2003, No. 24, item 198) and of 29 July 2005 (consolidated text: Journal of Laws of 2018, item 1030)	59,771	62,417
on copyright and related rights (consolidated text: Journal of Laws of 2022, item 2509)	11,285	3,285
on upbringing in sobriety and counteracting alcohol addiction (consolidated text: Journal of Laws of 2018, item 2137)	452	183
fiscal offences – Penal Fiscal Code	3,060	3,270

229. The list of categories of offences that may serve as predicate offences for money laundering is also published by the FATF[96]. These are: participation in an organised criminal group and racketeering; terrorism, including terrorist financing; trafficking in human beings and migrant smuggling; sexual exploitation, including sexual exploitation of children; illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking; illicit trafficking in stolen and other goods; corruption and bribery; fraud; counterfeiting currency; counterfeiting and piracy of products; environmental crime; murder, grievous bodily injury; kidnapping, illegal restraint and hostage-taking; robbery or theft; smuggling (including in relation to customs and excise duties and taxes); tax crimes (related to direct taxes and indirect taxes); extortion; forgery; piracy; insider trading and market manipulation. However, as explained by the FATF, it is up to each state to decide, in accordance with its national law, how it will define these offences and the nature of the various elements thereof.

[95] Statistical Yearbook of the Republic of Poland 2021, GUS, 2021, pp. 149-151, available at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/rocznik-statystyczny-rzeczypospolitej-polskiej-2021,2,21.html, and Statistical Yearbook of the Republic of Poland 2022, GUS, 2022, pp. 148-151, available at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/rocznik-statystyczny-rzeczypospolitej-polskiej-2022,2,22.html

[96] https://www.fatf-gafi.org/glossary/d-i/ access on 24.11.2021

230. The largest number of offences ascertained in 2020 were those against property, primarily fraud, i.e. offences penalised under Articles 286 and 287 of the Penal Code (133,202), accounting for approx. 17.0% of all ascertained offences. Offences related to theft or burglary and offences against the credibility of documents, i.e. offences referred to in Articles 270-277 of the Penal Code, were another numerous group.

231. However, the gravity of particular categories of offences should not be linked solely with the number of ascertained prohibited acts. In terms of counteracting money laundering, the specific characteristics of particular offences, related to the purpose of committing these offences and their impact on the level of public security, and above all, the total amount of assets that came into the possession of criminals as a result of committing these offences, are of key importance. For example, the Police, in its central KSIP data file (National Police Information System, that is a set of data files in which information, including personal data, is processed in connection with the implementation of the statutory tasks), records information about things related to the prohibited act and having features in the form of numbers enabling its clear identification. The Police records in the KSIP, among others, information on the amount of losses (damage) suffered as a result of the offence (in PLN)[97]. Losses in this case include material losses, the value of illegal trade, the value of financial gains or the amount of the public liability depletion. Losses should be understood as detriment to property caused directly by an offence, in particular through its seizure, damage, destruction or forfeiture. Losses are reported for offences committed (ascertained) upon completion of preparatory proceedings conducted by the Police. According to the data recorded in the KSIP for 2019-2021, the largest losses were recorded in the case of offences against property (a total of PLN 10.2 billion over three years), fiscal crimes (more than PLN 4 billion over three years), offences against economic transactions (a total of PLN 1.1 billion over three years), corruption offences (a total of PLN 226 million over three years), and offences related to the infringement of copyright and industrial property rights (a total of PLN 97 million over three years).

232. For example, one of the categories of offences as part of which the largest number of prohibited acts was ascertained in 2020 were offences against public security and traffic security, i.e. offences specified in Articles 163-180 of the *Penal Code* (72,958). It should be noted, however, that the vast majority of them (53,047) were prohibited acts related to driving a vehicle by a person under the influence of alcohol or drugs, i.e. those penalised under Article 178a of the *Penal Code*, that have no impact on the level of money laundering risk. Still the gravity of the offences referred to in Chapter XX of the *Penal Code*, included in the aforementioned category of offences, cannot be denied.

233. Predicate offences as well as money laundering are often detected and counteracted in the context of combating organised crime. The Central Investigation Bureau of the Police (CBŚP) data shows that in 2022, as a result of national and international activities carried out by the CBŚP to combat organised crime, the CBŚP eliminated a total of 181 (in 2019 – 182, in 2020 – 175, in 2021 – 177) criminal groups, including 161 (in 2019 – 161, in 2020 – 150, in 2021 – 163) Polish ones and 20 (in 2019 – 20, in 2020 – 24, in 2021 – 14) international ones[98].

[97] Article 30(1)(10) of the Order No. 70 of the Commander in Chief of the Police regarding the National Police Information System (KSIP) of 2 December 2019.

[98] Reports on the activities of the Central Investigation Bureau of the Police for 2019-2022 (a statistical approach), Central Investigation Bureau of the Police, at: https://cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

A large part of these groups were involved in drug and economic crime. Some of them were also involved in multi-crime activities.

234. Pursuant to the Act, the activities of the CBŚP are to limit the activity of economic criminal groups acting to the detriment of the State Treasury, and, above all, to combat the following predicate offences: VAT fraud and excise tax offences related to the illegal production and smuggling of cigarettes and imports of tobacco.

235. Brief descriptions of selected types of predicate offences for money laundering, arranged according to the gravity of a given category of offences in terms of estimates and available statistics relating to the amount of laundered money derived from these offences, are presented below.

236. Statistical data by predicate offence type is presented in Chapter 8. According to the presented data, the threat of crime is still high, in particular in the case of fiscal offences, various types of fraud/extortion, including those related to certifying an untruth or financial fraud, participation in an organised criminal group, and offences under the Act on counteracting drug addiction. The gravity of the threat of corruption must also be noted.

5.1.1. Fiscal offences

General characteristics

237. The *Act of 10 September 1999 – Penal Fiscal Code* (Journal of Laws of 2023, item 654), hereinafter referred to as the Penal Fiscal Code, penalises acts involving violation of prohibitions and orders specified in tax law, customs law, and foreign exchange law, as well as in the *Act of 19 November 2009 on gambling*[99]. A fiscal offence is an act prohibited under the Penal Fiscal Code on pain of a fine specified in daily rates, restriction of liberty or imprisonment.

238. The most recognisable fiscal offences include tax fraud related to tax on goods and services (VAT). Criminals use in this area the following *modi operandi* in various configurations:

- carousel fraud in intra-Community trade and fraud in intra-Community exports (the mechanism of carousel fraud is based on the fictitious flow (circulation) of goods between EU Member States and the creation of sham transactions through the circulation of invoices and other documents describing fictitious economic events),
- missing trader fraud,
- pretending intra-Community supplies or exports where unrecorded sales actually took place within the country,
- fraud involving a straw man issuing dummy VAT invoices that do not reflect actual economic events (where a missing trader is involved);
- abuse of customs procedure 4200[100].

[99] For information on fiscal offences involving illegal gambling see Chapter 5.1.6.
[100] Customs procedure 4200 relates to the exemption from value added tax on the import of goods dispatched or transported from a third territory or third country to a Member State other than that in which the dispatch or

239. Dummy invoices are issued both by existing entities running business and by fictitious entities, i.e. those that do not exist or exist only on paper and do not actually conduct business activity.

240. The purpose of VAT fraud is to:

- obtain an undue refund of the VAT difference,
- evade payment of a tax liability in whole or in part, while failing to disclose all or part of the business activity.

241. The experience of the CBŚP shows that the procedural and legislative solutions introduced since 2016 aimed at tightening the tax system have contributed to more effective identification of fiscal offences and their counteracting. These new solutions have resulted in, among others:

- a change in the *modus operandi* of organised criminal groups consisting in evading VAT by legally operating companies using the so-called "cost invoices" certifying fictitious economic events, whereas previously, this used to be mainly VAT carousel fraud with a missing trader involved,
- a decrease in the number of initiated cases and in the value of losses in these cases,
- however, despite the introduced systemic changes in the field of combating excise crime, criminal groups are still interested in tobacco crime due to significant financial gains.

242. Nonetheless, tax crime continues to be the dominant activity of groups dealing with economic crime in Poland.

243. VAT fraud includes fraud in international trade aimed at obtaining undue VAT refunds for fictitious transactions with foreign entities. The findings of detection and control activities carried out by the KAS bodies show that perpetrators often abuse industries that for years have been classified as high-risk ones due to the occurrence of tax irregularities, in particular in connection with the trade in products subject to excise duty. Excise goods are often also the subject of offences related to obtaining undue VAT refunds as well as failure to pay excise duty.

244. Since 2019, the involvement of criminal groups in the domestic illegal production of tobacco products has increased. In 2019, there was an over 35% increase in disclosed and seized tobacco products, a significant part of which was seized based on information provided by the CBŚP in other European countries, including the Kingdom of the Netherlands, Spain, the United Kingdom, Portugal and Slovakia, where illegal cigarette factories were located. A similar situation was recorded as regards dried tobacco. In this case, the quantity of the seized product increased by over 21% compared to 2018.

245. Since 2018, the Police have been recording increased activity of Polish criminal groups in other EU countries, which is due to, among others, the high effectiveness of the Police and other Polish services in combating fiscal crime related to the illegal manufacturing of tobacco products in Poland. Detection activities forced the organisers of this illegal practice to look for safer solutions and locations in other countries where they could pursue their activities. In this

transport of the goods ends 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).

respect, the high level of cooperation between CBŚP officers and representatives of law enforcement agencies of other countries, carried out directly or through EUROPOL, should be noted. A representative of the CBŚP is a national expert of SOC – AP SMOKE, an analytical project of EUROPOL, aimed to support the fight against organised international crime related to the illegal production, distribution and smuggling of excise goods. However, despite the high effectiveness of Polish services, criminal groups, counting on high profits, focus on the illegal manufacturing and distribution of tobacco products, which is reflected in the number (over 100) of illegal cigarette factories shut down in 2015 – 2020, as well as the quantity of tobacco products seized over the last few years. As regards the nationality of those involved in the illegal production of cigarettes and cut tobacco, the vast majority of them are Poles, most often acting as organisers and management staff. Other nationals directly involved in this illegal practice as mechanics and factory workers include Ukrainians, Belarusians and Armenians.

246. The market for cigarettes originating from criminal activity is supplied mainly by illegal factories. Nevertheless, there are occasional attempts to smuggle large amounts of cigarettes both by road, mainly from Belarus, and by sea. This data confirms previous trends related to Poland's geographical location, which means that we are still often a transit country through which tobacco products are transported to Western European markets.

247. Offences related to the illegal manufacturing of tobacco products are characterised by the fact that they are largely committed as part of the activities of organised criminal groups. This is due to their nature, requiring the involvement of a multi-person, organised structure, incurring specific financial outlays, and providing appropriate technical means (cigarette production machines, packaging for tobacco products, means of transport).

248. Fraud related to obtaining undue VAT refunds was most often prosecuted under Article 56 of the Penal Fiscal Code (regarding tax fraud) or under Article 62 of the Penal Fiscal Code (regarding violation of the accounting procedure).

Statistics

249. In 2022, heads of tax offices[101] initiated 22,187 (27,882 in 2021) preparatory proceedings in penal fiscal and criminal cases, including 6,036 (7,995 in 2021) preparatory proceedings in fiscal offence cases, 11,338 (14,482 in 2021) preparatory proceedings in fiscal misdemeanour cases, and 4,813 (5,405 in 2021) preparatory proceedings in cases of offences under the *Accounting Act*.

250. In 2022, heads of tax offices completed 25,661 (30,004 in 2021) preparatory proceedings in penal fiscal and criminal cases, including 7,587 (8,872 in 2021) preparatory proceedings in fiscal offence cases, 12,900 (15,923 in 2021) preparatory proceedings in fiscal misdemeanour cases, and 5,174 (5,209 in 2021) preparatory proceedings in cases of offences under the *Accounting Act*. In 2022, 63,564 (61,092 in 2021) fines were also imposed for a total amount of PLN 52,334,039 (PLN 35,328,809 in 2021).

Table 6. Preparatory proceedings conducted by heads of customs and tax control offices

Item	2020	2021	2022
Number of initiated preparatory proceedings	27,518	27,882	22,187

[101] Data: Report on the activities of the National Revenue Administration in 2021

Number of completed preparatory proceedings	26,168	30,004	25,661
Preparatory proceedings referred to court with an indictment	11,284	13,528	11,290
Preparatory proceedings referred to court with a request for permission to submit to liability on a voluntary basis	3,631	4,617	3,934
Preparatory proceedings ended with the imposition of a fine in the form of a penalty notice for fiscal misdemeanour[102]	4,378	5,593	4,697
Preparatory proceedings dismissed	5,657	5,056	4,717

251. In 2022, heads of customs and tax control offices[103] initiated 16.918 (14,758 in 2021) preparatory proceedings in penal fiscal and criminal cases, including 4,524 (5,598 in 2021) preparatory proceedings in fiscal offence cases, 10,743 (7,424 in 2021) preparatory proceedings in fiscal misdemeanour cases, and 1,651 (1,736 in 2021) preparatory proceedings in cases of common offences within the competence of the head of the customs and tax control office.

252. In 2022, heads of customs and tax control offices completed 17,492 (13,757 in 2021) preparatory proceedings in penal fiscal and criminal cases, including 5,786 (5,736 in 2021) preparatory proceedings in fiscal offence cases, 10,515 (6,994 in 2021) preparatory proceedings in fiscal misdemeanour cases, and 1,191 (1,027 in 2021) preparatory proceedings in cases of common offences. In 2022, 54,561 (40,697 in 2021) fines were imposed for a total amount of PLN 44,037,510 (PLN 23,766,131 in 2021).

Table 7. Preparatory proceedings conducted by heads of customs and tax control offices in 2020-2022

Item	2020	2021	2022
Number of initiated preparatory proceedings	18,735	14,758	16,918
Number of completed preparatory proceedings	16,878	13,757	17,492
Preparatory proceedings referred to court with an indictment	7,817	4,676	4,758
Preparatory proceedings referred to court with a request for permission to submit to liability on a voluntary basis	1,923	1,764	1,737
Preparatory proceedings ended with the imposition of a fine in the form of a penalty notice for fiscal misdemeanour[104]	157	344	2,056
Preparatory proceedings dismissed	2,362	2,349	2,718

253. The number of initiated penal fiscal and criminal proceedings reflects the activity of the National Revenue Administration in detecting violations of legal provisions, primarily tax and customs law. Actions taken in recent years to tighten the tax system have undoubtedly contributed to reducing the scale of law violations by taxpayers, which directly translates into a reduced number of disclosures of fiscal offences and fiscal misdemeanour. Besides changes in tax law, the tax system has been tightened also through the introduction into the *Penal Code* of penalties for forging VAT invoices, mainly the introduction of "VAT crime" into the *Penal Code*. The aforementioned changes in the *Penal Code* play an important preventive role and deter people from committing VAT offences. Moreover, in 2022, an external factor occurred in the form of the armed conflict in Ukraine, as a result of which the number of prohibited acts

[102] Applies to fines imposed under a penalty notice after initiation of preparatory proceedings.
[103] Data: Report on the activities of the National Revenue Administration in 2022 and Report of the National Revenue Administration in 2021
[104] Applies to fines imposed under a penalty notice after initiation of preparatory proceedings

disclosed at the Polish borders, that are also the external borders of the European Union, decreased. Therefore, the smaller scale of smuggling disclosures concerns mainly the Russian and Belarusian borders that remain largely closed to passenger and freight traffic. The statistically lower number of initiated preparatory proceedings was also due to their consolidation, e.g. in the area of gambling and VAT. However, it is worth noting a significant increase in 2022 compared to 2021, in the number of misdemeanour cases ended with the imposition of a fine, mainly in customs and tax control offices. This means that minor misdemeanour cases were dealt with quickly, without having to expend effort and resources to conduct preparatory proceedings, as a result of which more effort and resources could be put in more complex cases.

254. In 2022, the activities carried out by CBŚP officers resulted in shutting down 19 (also 19 in 2021) factories producing cigarettes as well as 17 (16 in 2021) plants where cut tobacco was produced. For comparison, both in 2020 and 2019, as a result of the activities of CBŚP units, 20 illegal cigarette factories were shut down in each of these years, 15 of which were located in Poland and the rest outside the Polish borders. As regards disclosures of illegal tobacco cutting plants, there were 15 such cases in 2020, i.e. 5 fewer than a year earlier, 14 of which concerned Poland and one the Czech Republic. In 2021, a record year in terms of the number of illegally produced cigarettes and tobacco seized, the CBŚP contributed to the seizure of a total of 280 million cigarettes and 541 tonnes of dried and cut tobacco.

255. According to Police data, as at the end of 2021, the CBŚP was conducting 254 (compared to 279 in 2020) preparatory proceedings in tax cases, which represented 60% (compared to 63% in 2020) of all cases dealt with by the division for combating organised economic crime at the CBŚP. There was a decrease in the number of cases in all categories, i.e. 177 investigations (compared to 191 in 2020) regarding VAT fraud, 33 cases (compared to 39 in 2020) regarding fuel crime, 40 proceedings (compared to 43 in 2020) regarding crime related to excise goods, and 4 cases (compared to 6 in 2020) regarding other tax matters. The value of property seized by the CBŚP in 2021 in economic cases conducted by this unit amounted to a total of PLN 543 million (compared to PLN 542 million in 2020), including PLN 332 million attributable to tax cases (compared to PLN 364 million in 2020).

256. According to information received from the Criminal Proceedings Division of the Internal Security Agency (ABW), this service conducted in 2019 – in the area of combating fiscal crime committed by organised criminal groups – 87 preparatory proceedings regarding money laundering, in which fiscal offences were predicate offences for money laundering. In 2020, the ABW conducted 81 such preparatory proceedings.

Examples of sanitised cases

Example 1

As part of an investigation conducted by the Lublin Branch of the National Prosecutor's Office in 2021, officers of the Central Investigation Bureau of the Police, National Revenue Administration and the Metropolitan Police Headquarters dismantled an organised criminal group and shut down an illegal cigarette factory where at least 25 million cigarettes could be produced per month. During the liquidation of the illegal cigarette factory, utility rooms and other facilities on the property were searched, as well as the suspects' places of residence. The officers seized cigarette manufacturing machines, compressors, a power generator and other

equipment, almost 5.6 million cigarettes, nearly 7.7 tonnes of cut tobacco, and components necessary for cigarette manufacturing. The officers seized also money, i.e. over PLN 1.4 million in various currencies found hidden in beds, cabinets and a fireplace. The devices included in the seized professional technological line for cigarette manufacturing are worth nearly PLN 2 million. A total of 11 suspects were detained (including 9 Belarusian citizens and 2 Poles) who were then arrested. It was established in the course of the investigation that the factory could produce 25 million cigarettes per month. The seized excise goods, i.e. cut tobacco and cigarettes, would have exposed the State Treasury to losses of at least PLN 15 million. The detainees were charged with participation in an organised criminal group and committing penal fiscal offences, i.e. production and marketing of excise goods.

Example 2

Under the supervision of the Lower Silesia Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Wrocław, an investigation has been conducted since 2019 regarding an organised criminal group whose members are suspected of certifying untruths in VAT invoices and tax documents to understate the taxes due. There are over 40 suspects in total in the case, accused of issuing fictitious invoices or using such documents to understate tax liabilities. The investigation is conducted by police officers from the Opole Branch of the Central Investigation Bureau of the Police together with officers of the Customs and Tax Control Office in Opole (KAS). According to the findings of the ongoing investigation, over 100 business entities may be involved in the criminal activity concerned. The group operated from 2017 to the early 2019. As a result of its activities, the State Treasury could suffer losses of over PLN 16 million. The investigation was carried out in several voivodeships. In the course of the operations, the officers searched the suspects' places of residence and the registered offices of the business entities, securing documents that were later analysed. The detainees were charged with participation in an organised criminal group and certifying untruths in VAT invoices. Pursuant to the Penal Code, this type of offence is punishable by imprisonment for up to 15 years. Movable property and real estate belonging to the suspects, worth a total of over PLN 3 million, was seized to cover future penalties and fines. The findings also show that the operators covered by the charges are filing corrections of their tax returns to tax offices and settling the understated taxes. Also in this case, the amounts of the corrected tax returns submitted so far exceed PLN 10 million.

5.1.2. Offences against property and economic transactions

General characteristics

257. Financial gains may also be derived from very common offences against property, i.e. theft (Article 278 of the Penal Code), theft with burglary (Article 279 of the Penal Code), misappropriation (Article 284 of the Penal Code), fraud (Article 286 of the Penal Code), or against economic transactions, e.g. causing damage in economic transactions (Article 296 of the Penal Code) or credit fraud (Article 297 of the Penal Code).

258. The most frequently committed offences against property in Poland include fraud under Article 286 of the Penal Code and credit fraud under Article 297 of the Penal Code. This act is often committed in multi-person configurations, whereby the perpetrators aim to make criminal activity their permanent source of income. Financial fraud as a predicate offence for money laundering identified and combated by the Police includes criminal methods consisting in:

- **cross-border fraud committed using investment platforms** – fraud is committed by people impersonating the so-called investment "brokers", i.e. employees of companies dealing with investment brokerage and advisory services. These companies advertise their services using social media, websites and mobile applications. To authenticate the content presented in advertisements, images of well-known and recognisable people are used, and the message is manipulated. Such entities operate without the necessary authorisations of the Polish Financial Supervision Authority and raise funds via investment platforms, that are later transferred abroad via subsequent bank accounts, making it difficult or impossible to recover the funds and determine the final beneficial owner. Transfers are often made at short intervals, i.e. within one day, funds can be transferred through several or a dozen different bank accounts, using fictitious accounts set up to carry out one or several transactions, at short intervals, for very high amounts, using the maximum number of fictitious elements, e.g. forged documents presented when opening an account, providing false purposes of opening an account or false purposes of ordered transactions. Cases of using anydesk software, enabling remote desktop control, have also been identified. Installing the software gives the perpetrator full control over the mobile device, i.e. a telephone or computer. When logging into a bank account, the criminal gains full access to the bank account. Funds extracted in this way are transferred through a chain of bank accounts opened for companies that do not conduct actual business activity or for straw men or persons with a false identity, making it difficult to determine the final beneficial owner. Business entities in such chain are most often registered in the name of foreigners, their addresses of these entities are not previously verified in any way and are located in virtual offices. Then the funds are transferred to foreign entities registered in tax havens, which ultimately makes it impossible to determine their beneficial owner,
- **fraud committed using Internet websites** – perpetrators, under the pretext of purchasing goods offered through a well-known Internet website, send a link redirecting to a confusingly similar website of a given platform with instructions to enter a payment card in order to allegedly quickly transfer money. In this way, criminals gain access to the seller's funds. The scammed funds are immediately transferred to new bank accounts set up for this purpose and then withdrawn. An increase involvement of Nigerian nationals was observed in committing this type of offences. Their task is to accept funds transferred to newly opened bank accounts to be further distributed through subsequent banking operations to the accounts of Chinese entities. Funds derived from crime can be legalised through the sale of goods that are difficult to count or whose value is difficult to estimate, such as know-how technology or a technological concept. Money entered in this way is transferred through the bank accounts of Polish and foreign business entities, which makes it difficult to determine its origin,
- **fraud using a false payment panel** – fraudulent behaviour consists in sending by perpetrators text messages with information about an alleged debt to be paid by the victim or the need to make an additional payment for a parcel delivery service. The text message includes a link that, when activated by the victim, redirects them to a website that looks like a real website of a bank or payment intermediary. Then the

victim unknowingly provides the perpetrators with their bank account login details, which enables the perpetrators to add a trusted payee profile and transfer funds from the victim's account to other bank accounts. The indicated accounts are most often set up in the name of straw men, fraudulently obtained money is transferred between different accounts to hide its criminal origin, and then withdrawn from ATMs or invested in cryptocurrency wallets,

- **advance-fee fraud** – the pattern of this fraud is constantly modified and includes, among others, **soldier or heir fraud**. In this scheme, the perpetrator most often contacts a random person via e-mail or instant messenger. In pursued correspondence, the perpetrator pretends to be a soldier/mercenary of the armed forces of a given country who has come into possession of significant assets or, alternatively, has come into a large inheritance. When exchanging correspondence, the perpetrator points to formal obstacles that prevent them from passing the funds or property onto the victim, e.g. the need to pay insurance for the shipment, costs related to legal advice, etc. In order to eliminate the obstacles, the victim makes payments to the indicated bank account or sends money using entities offering money transfers. Perpetrators most often operate using addresses of email boxes or instant messengers whose owners/service providers are based outside Poland. Fraudulently obtained funds are most often transferred to bank accounts opened for straw men and withdrawn using ATMs,
- **fraud in electronic payments** – due to ongoing technological and social changes, the number of non-cash transactions carried out via electronic transfers and card payments tends to increase. Criminals committing offences in the banking area use bank accounts opened with Polish banks remotely or with extremely limited physical contact with the bank branch:
  - EUR accounts kept for business entities show money transfers suspected of having no economic and legal rationale (the account are only used to be credited with funds from foreign natural persons that are then immediately transferred to entities that are difficult to identify – the countries where the business entities are established differ from those where the bank account is maintained, e.g. East Asian countries, tax havens),
  - the observed fraudulent scheme is similar to that used in investment fraud (company accounts are credited with funds from natural persons from Western Europe that are then transferred, within a few hours after they have been recorded, to the accounts of companies, most often IT or marketing ones, and the payment titles are imprecise and difficult to identify, e.g. payments for documents, payments for services).

259. This category of offences also includes pyramid schemes based on a Ponzi scheme.

Examples of sanitised cases

Example 1

In the spring of 2021, police officers from Gorzów Wielkopolski combating economic crime closed a case conducted under the supervision of the prosecutor's office, in which over 300

people were defrauded. The person suspected of the would buy jewellery on a Chinese website, usually for a dozen or so zlotys each, with the trademarks of a global manufacturer marked on it. Once purchased, the jewellery (chains, beads, pendants, etc.) was put up for sale in Poland at several times higher prices as original items. Sales took place online and the goods were delivered to people from various regions of Poland. The value of the original equivalents is at least PLN 100,000. A total of 337 fraud charges have been brought against the suspect. Besides fraud, the suspect will also be liable for trading in counterfeit trademarks and has also been charged with impersonating another person.

Example 2

Officers of the Katowice Regional Office of the Internal Security Agency, under the supervision of the Regional Prosecutor's Office in Katowice, concluded with an indictment an investigation into defrauding the Polish Agency for Enterprise Development (PARP) of a subsidy for a project of an innovative technology for generating electricity from industrial thermal waste. The total amount received by the company is almost PLN 12 million. In 2012, one of the companies concluded a project co-financing agreement with the PARP for almost PLN 29 million. The total funding actually provided to the company by the PARP was almost PLN 12 million. To obtain this amount, the company used, among others, forged invoices and invoices confirming work and services that had not actually been performed. The payment of the remaining funds awarded to the company has been suspended. The indictment covered three persons, including the president of the management board of the company that was the project beneficiary. The presented charges concerned the unfavourable disposal of the funds of the Polish Agency for Enterprise Development in the amount of over PLN 4 million, as well as fraud and issuing documents certifying untruths.

Example 3

In October 2020, officers of the Internal Security Agency detained two members of an organised criminal group involved in committing fiscal offences and VAT fraud in the trade in biofuels as well as laundering "dirty money" derived from this criminal activity. The estimated losses of the State Treasury amount to at least PLN 120 million. The fraudulent mechanism consisted in fictitious intra-Community acquisitions (ICA) of goods by Polish operators. The chains of recipients were purposefully and thoughtfully arranged so that some entities acted as missing traders and others as buffers to ultimately demonstrate the "lawful" purchase of rapeseed oil by final recipients, i.e. three companies registered in Poland. Then, through another company, the suspects took part in marketing vegetable oil in Poland, evading public law liabilities (VAT). This company, in which they were partners, was a link in the chain of entities supplying oil to other intermediary suppliers, and in some cases directly to the final recipient. The detainees were charged with participation in an organised criminal group and VAT fraud. The activities carried out by the officers of the Poznań Regional Office of the Agency of Internal Security in the above case also resulted in the issuance by the Regional Prosecutor's Office in Wrocław of decisions to seize the suspects' property in the total amount of PLN 527,000.

Example 4[105]

[105] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 roku (Report of the General

In 2020, the GIFI blocked a significant amount of funds on the accounts of a certain company and sent a notification in this case to the prosecutor's office. The case concerned defrauding a number of natural persons in connection with offering protective face masks. The accounts (in EUR and PLN) of a Polish company were credited with funds from natural persons and business entities. The transactions were described with transfer titles indicating orders for protective face masks. The total amount of funds that credited the said accounts exceeded several million PLN within 4 months. Part of the funds was transferred to another Polish company, then transferred to one of the Asian countries and withdrawn in cash abroad. The bank maintaining the accounts of the company concerned began to receive more and more messages from the banks of the transferors, requesting it to refund the funds, as well as complaints about the ordered transactions that could suggest fraud. A number of negative reports on transactions concluded with the company concerned were found in generally available databases. It could be concluded from the comments that a large number of people had been defrauded when purchasing protective face masks through the website that is no longer operational. The analysed company was not registered for VAT purposes and did not submit any tax returns to the Polish tax authorities throughout the period of its operation. The sole shareholder and at the same time the CEO of the company and the company itself were monitored by law enforcement agencies in connection with fraud.

5.1.3. Trafficking in narcotic drugs and psychotropic substances

General characteristics

260. Laundered funds may also originate from drug-related crime. The *Act of 29 July 2005 on counteracting drug addiction* (Journal of Laws of 2023, item 172) penalises, among others, the marketing of narcotic drugs, psychotropic substances and poppy straw or participation in the marketing thereof (Article 56). Providing another person with a narcotic drug or a psychotropic substance, facilitating the use or inducing the use of such a drug or substance in order to obtain financial gain shall also be punishable (Article 59). Moreover, in accordance with Article 61 of the aforementioned Act, anyone who, contrary to the provisions of the Act, Regulation 273/2004[106] or Regulation 111/2005[107], manufactures, processes, processes, imports, exports, carries out an intra-Community acquisition or intra-Community supply in order to illicitly manufacture a narcotic drug or a psychotropic substance shall also be penalised. The aforementioned types of prohibited acts are often committed within organised criminal structures, which results in more severe criminal liability.

261. According to the Police information for 2019 regarding organised drug-related crime in Poland, there were no significant qualitative changes compared to previous years. Poland was perceived as a transit country for smuggling significant quantities of cocaine (indirectly through ports in Belgium, the Kingdom of the Netherlands and Germany). Drugs are then transported overland back to Germany, Belgium, the Kingdom of the Netherlands or to

Inspector of Financial Information on the implementation of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2020), Warsaw, 2021, p. 47.

[106] 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).

[107] 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).

Scandinavian countries. In 2019, the upward trend in the imports of marijuana and hashish from countries such as Spain and France continued in Poland. Criminal groups used for this purpose mainly land and road transport.

262. 2020 was much different from previous years due to the restrictions introduced as part of the sanitary regime caused by the COVID-19 pandemic. However, despite difficulties related to movement, planning activities, ongoing implementation of previously developed plans and fulfilling new duties to ensure security and public order by police officers from the CBŚP – the number of drugs seized by the CBŚP Branches and Divisions increased compared to 2019. In 2021, the upward trend continued, and the quantities of narcotic drugs and psychoactive substances disclosed by the CBŚP remained at a high level. In 2021, the CBŚP seized in total over 11.36 tonnes of narcotic drugs and psychoactive substances (compared to 10.34 tonnes in 2020). In 2022, the quantity of disclosed narcotic drugs and psychoactive substances remained high, and the CBŚP seized a total of over 11.14 tonnes of these illicit goods. In the cases conducted by the CBŚP, approx. 7.88 (5.8 in 2021) tonnes of drugs were disclosed, and in the cases referred to other Police units (including foreign services) – approx. 3.26 tonnes (5.5 in 2021).

263. International organisations such as EUROPOL and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) also informed that the introduction of lockdown measures related to COVID-19 caused markets across the European region to shrink slightly or moderately due to disruptions in supply chains. This may be evidenced by a decline in narcotic drug seizures at borders and an increase in retail narcotic drug prices in some countries. There are indications that these market disruptions may have contributed to the revival of small-scale (home) production of synthetic drugs (amphetamine, methamphetamine, mephedrone) in some countries.

264. As far as logistics is concerned, organised criminal groups involved in drug-related crime made greater use of transport companies dealing with the transport of legal goods and moved their activities to the Internet. By operating online, they gained new distribution opportunities and could avoid face-to-face interactions. A large part of narcotic drugs was distributed via courier and postal items and picked by their recipients at collection points, which ensured their anonymity.

265. In Poland, as throughout Europe, the most popular narcotic drugs include marijuana and non-fibrous hemp products. All the time, despite the strict restrictions described above, there is still constant, significant supply of cocaine whose price, despite the increasingly higher quality, remains at a similar level. As in previous years, Poland was one of the main countries (apart from Belgium and the Kingdom of the Netherlands) producing amphetamine, and a transit country for heroin smuggled through Iran, Türkiye and Ukraine.

Table 8. Statistical data of the Border Guard regarding types of narcotic drugs detected and seized in 2020-2022[108]

Type of narcotic drug	Quantity			Value		
	2020	2021	2022	2020	2021	2022

[108] https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html, access on 11.04.2023

Total				**PLN 18,876, 940**	**PLN 46,623,501**	**PLN 28,135,414**
marijuana	327.4842 kg	494.7287 kg	425.8404 kg	PLN 11,454,687	PLN 21,936,032	PLN 18,985,075
amphetamine	18.3389 kg	129.3345kg 2 tabl.	44.3397 kg 17.5 l	PLN 807,696	PLN 9,295,397 PLN 50	PLN 3,085,481
hashish	50.7817 kg	245.8127 kg	0.6223 kg	PLN 2,529,153	PLN 12,290,615	PLN 1,084
heroin	0.0029 kg	0.0096 kg	0.0010 kg	PLN 282	PLN 1,828	PLN 240
cocaine	0.0847 kg	3.5311 kg	6.3728 kg	PLN 26,082	PLN 1,059,315	PLN 1,911,846
ecstasy	0.0103 kg 3,126.5 tabl.	0.3512 kg 10,318 tabl.	0.0395 kg 69 tabl.	PLN 345 PLN 31,506	PLN 10,132 PLN 362,466	PLN 1,499 PLN 2,090
psilocybin mushrooms	0.0858 kg		0.0027 kg	PLN 2,612		
LSD			268 pcs.			PLN 8,160
other				PLN 1,667,666	PLN 36,948,354	PLN 4,139,940

266. In 2021, the Border Guard initiated 277 preparatory proceedings[109] regarding drug-related crime. A total of 369 suspects, including 146 foreigners, were charged with committing an offence under the *Act on counteracting drug addiction*. 236 preparatory proceedings regarding this crime were completed. In 2022, the Border Guard initiated 195 preparatory proceedings regarding drug-related crime. 262 suspects, including 93 foreigners, were charged with committing an offence under the *Act on counteracting drug addiction*. 191 preparatory proceedings in this respect were completed.

267. In 2019, in cases conducted by the Central Investigation Bureau of the Police (CBŚP), a total of over 3,800 kg of various types of narcotic drugs, almost 30,000 ecstasy tablets and approx. 5,500 non-fibrous hemp bushes were detected and seized. Moreover, as a result of the activities undertaken by the CBŚP, over 7.2 tonnes of various types of narcotic drugs were seized, and 28 laboratories and 38 plantations were wound up. As regards cases conducted by the CBŚP in 2020, a total of over 10 tonnes of various types of narcotic drugs were detected and seized, and 31 laboratories and 75 plantations were wound up. As a result of the CBŚP activities in 2021, 40 synthetic drug laboratories and 43 professionally organised cannabis plantations were wound up, securing 7,276 (39,138 in 2020) cannabis bushes. In the cases conducted by the CBŚP, approx. 5.8 tonnes of narcotic drugs were disclosed, and in the cases referred to other Police units (including foreign services) – approx. 5.5 tonnes. Funds were also seized: in 2019 – PLN 31.2 million, and in 2020 – PLN 50.1 million. In 2022, the CBŚP wound up 42 synthetic drug laboratories and 20 professionally organised cannabis plantations, where 4,642 cannabis bushes were secured.

268. The National Revenue Administration (KAS) bodies also carry out inspections aimed at combating drug-related crime. In 2020, these bodies carried out 8,693 such inspections, as a result of which KAS officers made 1,799 disclosures of narcotic substances[110], substitutes and medicinal products. In 2019, 3,495 narcotic substances, substitutes and medicinal products were disclosed during 10,070 inspections. In 2020, cargo traffic was limited, the number of air

[109] Own data of the Border Guard
[110] Own data of the National Revenue Administration

shipments decreased, and air, road, sea and rail passenger traffic was limited due to the pandemic, which resulted in a lower number of disclosures of these substances.

Examples of sanitised cases

Example 1

Officers from the Krakow Branch of the Central Investigation Bureau of the Police (CBŚP) shut down a narcotic drug laboratory where amphetamine and BMK were produced. During the operation carried out in the Śląskie Voivodeship, three suspects, including a chemist, were detained. On the private real estate of one of the suspects, there were two technological lines for the production of amphetamine and its precursor, i.e. BMK. The laboratory was located in adequately prepared utility rooms and in the garage. In total, over 4 kg of solid amphetamine and 1.7 litres of liquid amphetamine were seized, which would be sufficient to generate over 13,000 dealer portions of amphetamine, worth nearly PLN 100,000. The police officers also found and seized nearly 1.3 kg of marijuana, 2.5 litres of a new psychotropic substance with a very strong action and over 2 litres of BMK, from which almost 2 kg of amphetamine could be produced. Excise goods were also found in one of the rooms. Officers of the Lesser Poland Customs and Tax Control Service (KAS) seized 890 kg of cut tobacco. The KAS officers took over the excise tax issue in this case for clarification. The prosecutor brought charges against the detained group members for producing significant amounts of psychotropic substances. Based on the collected evidence, at the request of the prosecutor, the court imposed a preventive measure on the group members in the form of temporary detention for 3 months.

Example 2

The Regional Prosecutor's Office in Koszalin charged two men with possession of significant amounts of narcotic drugs and psychotropic substances. This type of offence is punishable by up to 10 years in prison. The District Court in Koszalin, based on the material collected by officers from the Szczecin Branch of the Central Investigation Bureau of the Police, applied preventive measures with respect to both suspects in the form of temporary detention for 3 months. During the search of the flats, utility rooms, buildings and cars used by the suspects, the officers found and seized a total of over 13 kilograms of marijuana, over 5 kilograms of amphetamine, as well as scales and other devices used for portioning and packaging narcotic substances. During their operations, the police officers also seized two weapons. The street value of the seized narcotic drugs is estimated at nearly PLN 300,000.

5.1.4. Corruption

General characteristics

269. 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 Penal Code. A separate regulation is also provided for in the *Act of 25 June 2010 on sports* (Journal of Laws of 2022, item 1599) that penalises corruption acts connected with sports competitions, and the *Act of 12 May 2011 on reimbursement for medicines, foodstuffs for particular nutritional uses and medical devices* (Journal of Laws of 2023, item 826), penalising corruption acts related to the trade in medicines, foodstuffs for particular nutritional uses and medical devices. The nature of the corruption offence is reflected in the definition of corruption contained in Article 1(3a)

of the *Act of 9 June 2006 on the Central Anti-Corruption Bureau* (consolidated text: Journal of Laws of 2022, item 1900, as amended). Corruption, within the meaning of this Act, is an act:

(1) consisting in promising, proposing or giving by any person, directly or indirectly, any undue benefits to a person performing a public function for themselves or for any other person, in exchange for action or omission to act in the performance of their function;

(2) consisting in demanding or accepting by a person performing a public function, directly or indirectly, any undue benefits for themselves or for any other person, or accepting an offer or promise of such benefits, in exchange for action or omission to act in the performance of their function;

(3) committed in the course of business activity including the fulfilment of obligations towards a public authority (institution), consisting in promising, proposing or giving, directly or indirectly, to a person managing an entity not included in the public finance sector or working in any capacity for such an entity, any undue benefits, for themselves or for any other person, in return for an action or omission of an action that violates their obligations and constitutes socially harmful reciprocity;

(4) committed in the course of business activity including the fulfilment of obligations towards a public authority (institution), consisting in demanding or accepting, directly or indirectly, by a person managing an entity not included in the public finance sector or working in any capacity for such an entity, any undue benefits or accepting an offer or a promise of such benefits for themselves or for any other person, in return for an action or omission of an action that violates their obligations and constitutes socially harmful reciprocity.

270. The most common predicate offences from which financial gains subject to laundering originate include bribery. Any person who gives or promises to give a bribe in exchange for the handling of a matter of interest to them in an office or institution by a person receiving a material or personal benefit or a promise thereof may the subject of active bribery. Any person who, in connection with the performance of a public function, accepts a material or personal benefit or a promise thereof, or a person who is not a public official but performs a public function and accepts (takes) a bribe may be the subject of passive bribery (venality).

271. Public officials include the persons indicated in Article 115(13) of the Penal Code, i.e.:

- President of the Republic of Poland,
- MP, senator, councillor,
- Member of the European Parliament,
- judge, lay judge, prosecutor, officer of the financial body of preparatory proceedings or of the body superior to the financial body of preparatory proceedings, notary, bailiff, probation officer, trustee, court supervisor and administrator, person adjudicating in disciplinary bodies operating under the Act,
- a person who is an employee of government administration, another state body or a local government body, unless they perform only service activities, as well as another person in so far as they are authorised to issue administrative decisions,

- a person who is an employee of a state control body or a local government control body, unless they perform only service activities,
- a person holding a managerial position in another state institution (i.e. heads of institutions, their deputies, heads of departments and divisions),
- an officer of a body responsible for protecting public security (e.g. the Police, Internal Security Agency, Border Guard) or an officer of the Prison Service,
- a person performing active military service, with the exception of territorial military service performed on an as available basis,
- an employee of an international criminal tribunal, unless they perform exclusively service activities.

272. Pursuant to Article 115(19) of the Penal Code, persons performing public functions include public officials, members of local government bodies, persons employed in organisational units having public funds at their disposal, unless they perform only service activities, as well as other persons whose rights and obligations in the field of public activity are defined or recognised by an act or an international agreement binding on the Republic of Poland. Persons performing exclusively service activities do not exercise the substantive competence of a given body, are not authorised to manage or make decisions in this regard, but only facilitate the work of this body.

273. A financial benefit is any good that is able to satisfy a specific need and its value can be expressed in money. It may be not only an increase in assets, but also any beneficial contracts, e.g. a loan granted on favourable terms.

274. A personal benefit is a non-pecuniary benefit that improves the situation of the person who receives it (e.g. a promise of a promotion, decoration with an order, training in a profession).

Statistics

275. The Concise Statistical Yearbook of Poland issued in 2022[111] by Statistics Poland included corruption offences in the part regarding "offences ascertained by the Police and the Prosecutor's Office in completed preparatory proceedings". According to the data presented in the aforementioned document, a total of 8,340 corruption offences (including those specified in Articles 228 - 231, 250a, 296a and 296b of the Penal Code) were committed in 2021 (compared to a total of 10,438 in 2020). The largest number of proceedings were conducted by the Police – a total of 6,370 (compared to 8,038 in 2020). According to data for 2019 presented in the Concise Statistical Yearbook of Poland published in 2020, a total of 9,367 corruption offences were committed in 2019.

276. The CBA, as a service dedicated to combating corruption in public and economic life, initiated 228 preparatory proceedings in 2022 (165 in 2021)[112] (106 ones were conducted based on its own materials, and 122 based on materials entrusted by the prosecutor's office). In 2022,

[111] https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/roczniki-statystyczne/maly-rocznik-statystyczny-polski-2022,1,24.html, access on 11.04.2023

[112] Information on the outcomes of the activities of the Central Anti-Corruption Bureau in 2021 and Information on the outcomes of the Central-Anti Corruption Bureau in 2022, https://www.cba.gov.pl/pl/o-nas/informacja-o-wynikach, access on 21.04.2023

the CBA conducted a total of 694 (584 in 2021) proceedings and completed 208 (158 in 2021) of them. As a result, 869 (688 in 2021) suspects were charged for the first time. A total of 3,101 (2,020 in 2021) charges were presented in the conducted proceedings.

277. In the course of the preparatory proceedings conducted by the CBA in 2022, property[113] with a total value of over PLN 232.38 million, over EUR 62.7 thousand and USD 44.8 thousand was seized (over PLN 228.2 million, EUR 149 thousand and USD 184.48 thousand in 2021). In the course of operational and reconnaissance activities carried out in 2022, it was found that State Treasury lost PLN 390.15 million (PLN 4,568.5 million in 2021), while the value of disclosed material benefits amounted to PLN 12.74 million (PLN 288.2 million in 2021).

278. As far as the ownership structure of the receiving entity is concerned, corruption can be classified as occurring in the public, private or public-private sector. In 2018, the number of preparatory proceedings by sector[114], taking into account the percentage of the total number of 1,229 proceedings (according to the methodology adopted for the report "Areas of corruption crime in Poland in 2018-2019"), was as follows:

Table 9. Number of preparatory proceedings in corruption cases by sector (taking into account the ownership structure of the receiving entity) in 2018

Public sector	895	72.8%
Private sector	194	15.8%
Public-private sector	140	11.4%

279. Based on the data from the aforementioned report and the number of conducted proceedings, it can be assumed that in approx. 73% of corruption cases, the recipient was a representative of the public sector, which means that corruption in the public sector occurred twice as often as in the private and public-private sectors. The above report also includes an analyses by area of activity of the entity receiving the benefit. It shows that preparatory proceedings in two areas alone, i.e. the "public administration" area and the "law enforcement agencies and justice authorities" area, account for more than half of all preparatory proceedings.

280. In 2021, the Central Anti-Corruption Bureau (CBA) conducted 59 preparatory proceedings (including 15 initiated in 2021) in which money laundering – Article 299 of the Penal Code – was the main qualification. During this period, the CBA also conducted 74 proceedings in which one of the charges included a qualification under Article 299 of the Penal Code. A total of 96 charges were filed in connection with these proceedings.

281. According to information received from the Criminal Proceedings Division of the Internal Security Agency (ABW), this service conducted in 2019 – in the area of combating corruption crime – 4 preparatory proceedings regarding money laundering, in which corruption offences were predicate offences for money laundering. In 2020, the ABW conducted 3 such preparatory proceedings.

[113]Ibidem

[114] Report of the Central Anti-Corruption Bureau "OBSZARY PRZESTĘPCZOŚCI KORUPCYJNEJ W POLSCE W LATACH 2018-2019" (CORRUPTION CRIME AREAS IN POLAND IN 2018-2019), https://www.cba.gov.pl/pl/antykorupc/publikacje/publikacje-w-jezyku-po/4387, Obszary-przestepczosci-korupcyjnej-w-Polsce-w-latach-20182019.html, access on 08.12.2021

Examples of sanitised cases

Example 1

Corruption in the army

As a result of the cooperation of the Central Anti-Corruption Bureau (CBA) and Military Police officers, evidence was collected, based on which an investigation was initiated into irregularities in connection with the organisation of tenders for the purchase of equipment and services for the army, which could expose the State Treasury to significant losses. The findings showed that in 2018-2019, tender collusion and corruption offences involving soldiers responsible for conducting tenders and individuals running businesses occurred.

Example 2

Activities to the detriment of a company

In 2020, CBA officers continued preparatory proceedings regarding activities to the detriment of a development company implementing major construction projects. The detainees were involved in siphoning money from the company by appropriating large amounts of entrusted funds and then putting them into legal circulation. The criminal mechanism consisted in purchasing fictitious receivables to the detriment of the managed company and transferring funds via a number of business entities to the accounts of Polish and foreign entities indicated by the organisers. The company's loss was estimated at over PLN 60 million. A total of 12 individuals were detained. Preventive measures other than deprivation of liberty were applied to 6 suspects

Example 3

Unfavourable disposition of property in a ministry

The case concerned unfavourable disposition of EU funds in the Ministry of Infrastructure and Development in connection with the implementation of projects supervised by one of the voivodeship labour offices in 2012-2013 using false documents. As part of the investigation, evidence covering a total of 21 EU projects financed by the ESF under the Human Capital Operational Programme was secured. Charges were brought against 31 suspects. In July 2020, an indictment was filed in the case against 18 individuals. One of the suspects was accused of, among others, causing an unfavourable disposition of property worth almost PLN 1.5 million to the detriment of the Education Development Centre of the Ministry of National Education and the Voivodeship Labour Office, as well as an attempt to cause an unfavourable disposition of property worth a total of over PLN 154,000 to the detriment of the Centre.

282. Poland is a signatory to the OECD Convention of 21 November 1997 on Combating Bribery of Foreign Public Officials in International Business Transactions – a joint commitment of the governments of leading industrialised countries doing business with foreign investors[115]. The Convention entered into force in 1999. It is the first international legal instrument focused on the "supply party" in a corrupt transaction, i.e. a person or entity that offers, promises or gives a bribe. The Convention obliges the signatory states to criminalise bribery of foreign public officials. The offence of bribery of a foreign public official is defined in the Convention

[115] https://antykorupcja.gov.pl/ak/aktualnosci/11269,Antykorupcyjna-Konwencja-OECD.html, access on 25.04.2023

as “intentional offering, promising or giving by any person any undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official, for that official or for a third party, in order that the official act or refrain from acting in relation to the performance of official duties, in order to obtain or retain business or other improper advantage in the conduct of international business”. Since the Convention entered into force, there has been only one case in Poland of a conviction for corrupting foreign officials. The criminal proceedings concerned the period from April 2009 to March 2010. A Polish citizen authorised a Polish intermediary to pay bribes of EUR 65,000 to a German customs officer in order to falsify export documents. In Germany, both the official and the intermediary were sentenced to four years in prison. In Poland, the proceedings were based on evidence collected by German authorities and concerned the Polish citizen. In December 2012, the Polish citizen was convicted of foreign bribery (Article 229(5), Article 229(3) and Article 229(4) of the Penal Code) to imprisonment for two years and fined approx. EUR 8,500. The prison sentence was conditionally suspended for a five-year probation period.

283. A foreign bribery offence may be detected through media reports, reporting by Polish public officials, reporting through foreign diplomatic missions or through accounting and auditing. Irregularities may also be reported by whistleblowers. Foreign bribery may be detected, among others, using anti-money laundering instruments. Laundering of money originating from corruption or misappropriation of property by foreign public officials has been long reflected in the applications received by the GIFI from foreign financial intelligence units. In 2022, the GIFI recorded a total of 18 applications regarding potential laundering of money originating from embezzlement and 5 applications regarding funds potentially derived from corruption. 87% of applications were submitted by the GIFI’s foreign partners from outside the European Union, mainly from the former Soviet Union.

284. As regards the offence of bribery of a foreign public official, Poland was evaluated by the OECD Working Group on Bribery in International Trade Transactions[116]. According to data from the final report on this evaluation, six known foreign bribery allegations against Polish persons or companies have been recorded in Poland since 2013. Only one of these six cases was successfully prosecuted. One case is pending and one is suspended. In another case, the charge concerned ultimately embezzlement, not foreign bribery. Two allegations of foreign bribery were not properly investigated.

285. Combating foreign corruption is extremely difficult in every country that is a party to the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. In Poland, one criminal proceeding regarding the possible involvement of Polish entities in this type of offence is pending. The proceeding concern a case in which, between October 2016 and October 2019, Ukrainian, Turkish and Polish companies allegedly bribed the head of the Ukrainian state agency Ukravtodor. This person is a Polish citizen. The alleged bribes of a total of approx. EUR 1 million concerned road reconstruction contracts. The case also involved the laundering of money derived from bribery that took place from 1 November 2016 to 30 September 2019 in Poland and Ukraine. In July 2020, 16 individuals were charged with various offences, including four charged with active bribery of a foreign officer (Article 229(1) and (5) of the Penal Code). One person was convicted of money laundering and

[116] The evaluation concerned the fourth assessment of Poland’s implementation of the *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*

complicity in passive foreign bribery. As a result of an investigation conducted jointly by the National Anti-Corruption Bureau of Ukraine and the Polish Central Anti-Corruption Bureau, the main suspect in the proceedings was accused of receiving financial benefits or accepting promises of such benefits in an amount equivalent to over PLN 6.1 million, participating in the laundering of money in the amount of approx. PLN 8 million, and committing minor corruption acts in Poland.

5.1.5. Human trafficking and migrant smuggling

General characteristics

286. In the Polish *Penal Code*, the offence of human trafficking is regulated in Article 189a that penalises this prohibited act with imprisonment for a period of not less than 3 years. Preparation to commit this act is also punishable. Pursuant to Article 115(22) of the *Penal Code*, human trafficking includes the recruitment, transportation, delivery, transfer, harbouring or reception of a person by means of violence or unlawful threat, abduction, deceit, misinformation or exploitation of an error or inability to properly understand the undertaken action, abuse of a relationship of dependence, taking advantage of an urgent plight or the position of vulnerability, granting or accepting a material or personal benefit or promising such benefit to a person taking care of or having control over another person for the purpose of their exploitation, even with their consent, in particular in prostitution, pornography or other forms of sexual exploitation, forced labour or services, including begging, slavery or other forms of exploitation degrading human dignity, or for the purpose of obtaining cells, tissues or organs contrary to the provisions of the Act. If the perpetrator's conduct involves a minor, it is classified as human trafficking, even where the methods or means listed in subparagraphs 1-6 of this provision have not been used.

287. Migrant smuggling is penalised in Article 264(3) of the *Penal Code*, where organising the crossing of the border of the Republic of Poland by other people is punishable by imprisonment. The border of the Republic of Poland (referred to, in the *Act of 12 October 1990 on the protection of the state border* (Journal of Laws of 2022, item 295), as the "state border") is the vertical area passing through the border line separating the territory of the Polish state from the territories of other countries and from the high sea. The state border also delimits airspace, waters and the interior of the earth. The course of the state border on land and the delimitation of internal sea waters and the territorial sea with neighbouring countries are specified in international agreements concluded by the Republic of Poland. The state border at sea runs at a distance of 12 nautical miles (i.e. 22,224 m) from the baseline, specified in other regulations, or along the outer border of the roadsteads incorporated into the territorial sea. The rules for the legal crossing of the border of the Republic of Poland are specified in the *Act on the protection of the state border*. They are also specified in the *Schengen Borders Code*[117] (Article 14(3)) that states that the crossing of the state border constituting an internal border within the meaning of this Code is permitted through border crossings intended and open for border traffic, subject to the provisions of international agreements binding on the Republic of Poland.

[117] REGULATION (EU) 2016/399 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)

288. In some countries, both offences are often a source of significant income for criminal groups engaged in such activities. The difference between human trafficking and migrant smuggling is that human trafficking usually involves the use of force, coercion, deception or other abuse that includes an element of exploitation and renders the victim's consent irrelevant. Individuals or criminal groups involved in human trafficking profit from exploiting their victims, while in the case of smuggling humans across the border, migrants pay smugglers to help them cross the border illegally. Usually, after arriving at the destination, further contacts between the smuggler and the migrants cease.

289. In the face of the ongoing armed conflict in Ukraine and the resulting wave of refugees from Ukraine to Poland (and other countries), the Polish legislator amended the *Act of 12 March 2022 on assistance to citizens of Ukraine in connection with the armed conflict in the territory of this state* (Journal of Laws of 2023, item 103) by introducing Article 72 therein to increase penalties for offences related to human trafficking and prostitution-related offences committed to the detriment of refugees. Pursuant to the aforementioned provision, in cases of convicting a perpetrator who committed the offence of human trafficking (referred to in Article 189a(1) of the *Penal Code*) during the armed conflict in the territory of Ukraine, courts are obliged to impose a penalty in the form of deprivation of liberty for a period from 10 to 15 years or 25 years. So far, such perpetrator was subject to the penalty of imprisonment for a period of not less than 3 years. The increased penalties adopted by the Sejm are to deter criminals from committing this type of offences against refugees from Ukraine.

290. Due to different data collection methodologies adopted by entities dealing with human trafficking, statistics related to this illegal practice may vary. The picture of the phenomenon concerned is completed with information from non-governmental organisations cooperating with law enforcement agencies and the justice system in supporting victims of this offence. Due to its geopolitical location, Poland – as far as human trafficking is concerned – is also a country of origin, transit and destination for victims of human trafficking. Polish citizens, both women and men, may be recruited in Poland and then exploited for forced labour, prostitution, begging, theft or extracting benefits and loans abroad. Poland may also be a destination for organisers of human trafficking. In this sense, foreigners are exploited in Poland. Victims most commonly include citizens of European countries: Ukraine, Bulgaria, Belarus and Romania, as well as Asian countries (including Vietnam, the Philippines, Sri Lanka) and Latin America (including Mexico, Colombia, Venezuela). Foreigners are exploited for forced labour, prostitution, begging, and sometimes they are also victims of domestic slavery and criminal exploitation. The year 2020 seems to confirm that the use of people for forced labour has been the prevailing form of human trafficking for several years[118].

Statistics

291. As regards human trafficking, in 2016 - 2020, the Police[119] conducted the following number of proceedings under Article 189a of the *Penal Code*:

[118] 2020 Report on Trafficking in Human Beings, https://www.gov.pl/web/handel-ludzmi/handel-ludzmi-w-polsce-raport-2020

[119] https://statystyka.policja.pl/st/wybrane-statystyki/handel-ludzmi-i-przest/50848,Handel-ludzmi-i-przestepstwa-okoloprostytucyjne.html, access on 10.12.2021

Table 10. Human trafficking – Article 189a(1)-(2) of the Penal Code (number of proceedings in 2016-2020)

Human trafficking – Article 189a(1)-(2) of the *Penal Code*				
Year	Proceedings initiated	Proceedings completed	Offences ascertained	Offences detected
2020	14	22	11	11
2019	16	32	25	23
2018	33	42	67	64
2017	27	36	85	82
2016	31	38	9	7

292. As regards forced prostitution, in 2016 – 2020, the Police conducted the following number of proceedings under Article 203 of the *Penal Code*:

Table 11. Number of proceedings regarding forced prostitution in 2016 - 2020

Forced prostitution – Article 203 of the *Penal Code*				
Year	Proceedings initiated	Proceedings completed	Offences ascertained	Offences detected
2020	11	11	12	12
2019	13	15	12	12
2018	14	26	25	24
2017	17	15	28	27
2016	14	26	25	20

293. As regards procurement, pimping and facilitation of prostitution, also involving minors, in 2016 - 2020, the Police conducted the following number of proceedings under Article 204(1)-(3) of the *Penal Code:*

Table 12. Number of proceedings regarding procurement, pimping and facilitation of prostitution in 2016-2020

Procurement, pimping and facilitation of prostitution, also involving minors – Article 204(1)-(3) of the *Penal Code*				
Year	Proceedings initiated	Proceedings completed	Offences ascertained	Offences detected
2020	64	77	191	187
2019	64	75	107	107
2018	79	101	191	183
2017	91	110	247	243
2016	74	109	357	337

294. As part of its statutory powers, the Border Guard carries out controls of the legality of employment of foreigners, running a business by foreigners, and entrusting work to foreigners (controls of legality of employment). Regular controls of the legality of employment are a real tool to mitigate exploitation for forced labour and deriving illegal income from it.

Table 13. Number of controls of the legality of employment conducted by the Border Guard in 2019-2022

Number of controls of the legality of employment carried out by the Border Guard in 2019-2020					
Year	Number of conducted controls	Number of controls where violations were identified	Number of foreigners covered by controls	Number of foreigners with respect to whom violations were identified	Number of employers who entrusted work illegally
2019	4,094	3,576	124,979	14,740	2,403
2020	2,361	2,052	65,893	8,185	1,428
2021	2,216	1,895	91,922	9,938	1,184
2022	1,941	1,683	72,623	11,401	1,408

Violations were found mainly with respect to citizens of Ukraine, Belarus, Georgia, and Moldova, and to a lesser extent – Russia, India, Bangladesh, Vietnam, Türkiye, Nepal, Uzbekistan and the Philippines.

In 2020, the Border Guard initiated 8 new investigations in the area of human trafficking: 5 in the area of exploitation for forced labour; 2 in the area of exploitation for prostitution, and 1 relating to other forms of exploitation degrading human dignity. In the course of investigations conducted in 2020, one suspect (a Polish citizen) was charged with trafficking in human beings[120]. In 2021, Border Guard officers initiated 12 investigations into human trafficking crime: 7 relating to exploitation for forced labour; 3 relating to exploitation for prostitution, 1 relating to forced begging, and 1 relating to other forms of exploitation (marriage of convenience). Charges with respect to the aforementioned offences was brought against 5 suspects, including 4 citizens of the Republic of Poland and 1 citizen of Yemen. In 2021, the Border Guard completed 7 proceedings – in two cases indictments were brought, while the remaining 5 proceedings were discontinued. Based on statistical data on the number of identified victims and preparatory proceedings initiated by the Border Guard, forced labour continues to be the dominant form of exploitation. In 2021, the Border Guard identified a total of 71 alleged victims of human trafficking, most of whom were used for forced labour. The victims most often came from: Colombia (25), Moldova (14), Mexico (9), and Venezuela (6). In 2022, the Border Guard identified a total of 110 alleged victims of human trafficking. 106 as part of 4 investigations into exploitation for forced labour: 38 citizens of Guatemala, 37 citizens of Venezuela, 15 citizens of Mexico, 15 citizens of Colombia, and 1 citizen of Honduras. The following single cases of victims of human trafficking were also identified: 1 citizen of Ukraine – forced labour/domestic slavery, 1 citizen of Cameroon – exploitation for prostitution, 1 citizen of Congo – exploitation for prostitution, 1 citizen of Russia – exploitation for begging.

295. According to data provided by the National Prosecutor's Office in 2020, the most common forms of exploitation included forced labour or services, as well as prostitution and

[120] 2020 Report on Trafficking in Human Beings, https://www.gov.pl/web/handel-ludzmi/handel-ludzmi-w-polsce-raport-2020

other forms of sexual exploitation. Cases of marriages of convenience, child trafficking, and tissue or organ harvesting were also reported. In 2020, the number of victims of human trafficking was 269, including 8 minors[121].

296. As regards all offences relating to illegal border crossing, in 2016 – 2020, the Police conducted the following number of proceedings under Article 264 of the *Penal Code*:

Table 14. Number of cases of illegal border crossing in 2016-2020

Crossing the border illegally (Article 264)		
Year	**Number of proceedings initiated**	**Number of offences ascertained**
2020	2	3
2019	4	9
2018	2	3
2017	2	9
2016	4	2

297. In 2021, Poland experienced growing migration pressure from third-country nationals on the Polish-Belarusian section of the state border, that is also the external border of the European Union and the Schengen area. These foreigners legally entered the territory of Belarus by air and then attempted to illegally cross the Polish border and enter the territory of Poland. These activities were supported by the Belarusian state services. These services coordinated providing foreigners with accommodation and food and their transport to the state border with the European Union, for which they collected significant amounts of money from each person. These actions seemed to be aimed at destabilising the situation in the territory of the Republic of Poland and the European Union. According to the Border Guard data, in 2021, a total of 39,697 third-country nationals[122] attempted to illegally cross the Polish state border along the Belarusian section outside official border crossings. This represents an over 300-fold increase compared to 2020. According to data available to the Border Guard, in 2020, in the same period, only 129 people tried to illegally cross the state border with Belarus outside official border crossings. A sharp increase in attempts to illegally cross the Polish-Belarusian border was recorded since August 2021. The peak of the migration crisis occurred in October 2021, when a total of 17,447 such attempts were recorded. The number of attempts to illegally cross the state border with Belarus decreased significantly in November 2021 – 8,917, and in December 2021 – 1,740. The Border Guard Post in Michałów faced the greatest migration pressure. In the section protected by it, 5,466 foreigners tried to cross the border illegally. A large number of such attempts also took place in the area of the Border Guard Post in Mielnik – 4,890 foreigners, and the Border Guard Post in Białowieża – 4,855 foreigners. As far as the nationality of the foreigners crossing the state border is concerned, these were most often citizens of Iraq, Afghanistan, Syria, Russia, Somalia, Tajikistan, Iran and Türkiye (their migration is facilitated by a large number of direct air connections between Minsk and Istanbul, Moscow, Baghdad and Dubai). Polish border services also detained individuals responsible for the transfer of

[121] 2020 Report on Trafficking in Human Beings, https://www.gov.pl/web/handel-ludzmi/handel-ludzmi-w-polsce-raport-2020

[122] https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html, access on 11.03.2022

migrants through the Polish territory (these people would arrive at the border to pick up illegal migrants and transport them farther in Poland or to Western Europe).

298. In 2022, the Border Guard detained a total of 5,471 foreigners for crossing or attempting to cross the state border illegally or disclosed such foreigners, while in 2021, this figure was 10,458[123]. In 2020, 4,156 such detentions/disclosures were reported. At the external border of the European Union (including Russia, Belarus, Ukraine, external sea connections and external air connections), there were 2,815 such detentions/disclosures in 2022, 7,463 in 2021, and 2,361 in 2020. At the internal border of the European Union, these figures for 2022, 2021 and 2020 were 2,656, 2,995 and 1,795, respectively.

Examples of sanitised cases

Example 1

The investigation – supervised by the Regional Prosecutor's Office in Gdańsk – ended with filing an indictment to the court, was conducted by the Maritime Branch of the Border Guard in Gdańsk. The prosecutor charged the main defendant with the offence of human trafficking, as well as appropriation of property of a significant value, inciting others to assault, threatening with assault, causing grievous bodily harm and destroying property. During the investigation, it was found that Euzebiusz D., the accused, used his legal business activity to recruit people to work in Poland and Sweden. He cooperated with many companies to which he referred the recruited people to work in the construction industry. Recruitment took place mainly through advertisements posted on Polish and Ukrainian websites. The recruited people were not provided with decent living conditions either in Poland or Sweden and worked illegally. Even though the companies for which the work was performed provided the defendant with money for remuneration, it was not paid at all or it was paid in amounts that were insufficient to meet the workers' needs. The workers' remuneration was reduced with amounts for housing, alleged insurance and workwear. Threats of financial penalties and expulsion from the country were used to force the workers to obey orders. They were also threatened that in case of their escape, they would be found together with their families and would face consequences The victims were mainly Ukrainian citizens. It was established that the accused forced to work at least 100 people. He also appropriated the remuneration due to the workers in an amount of at least PLN 2,988,000.00. The money transferred by the companies for the workers' wages was transferred to the bank accounts of business entities managed by two defendants. In order to conceal the origin of the money, the defendants made dozens of transfers between several accounts.

Example 2

In March 2021, the Regional Prosecutor's Office in Sosnowiec brought an indictment to the Regional Court in Katowice against two men (32- and 38-year-old) who were accused of committing the offence of human trafficking and benefiting from prostitution. The accused were

[123] INFORMACJA STATYSTYCZNA za 2021 r. Komendy Głównej Straży Granicznej (STATISTICAL INFORMATION for 2021 of the Border Guard Headquarters), Warsaw, January 2022, https://strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html, access on 11.03.2022

arrested in 2020 by police officers from the Katowice voivodeship headquarters dealing with combating human trafficking. An 18-year-old woman, in an extremely difficult life and financial situation, was looking for a job. One of the suspects, under the guise of employing her in a restaurant, arranged for her to meet a 38-year-old man. The woman found out what her job was when the men took her to a flat in Katowice, where an informal escort agency was located. From March to August 2015, the victim, under the supervision of the 38-year-old man, provided sexual services in a flat rented by him. From time to time, the man changed her place of stay and took her to other flats in Katowice, Sosnowiec and Cieszyn, where he organised her meetings with clients. In 2015 - 2017, the victim was exploited for prostitution in the United Kingdom and later in Germany. The suspects forced the woman to provide sexual services, using physical and psychological violence against her. They also derived financial benefits from the illegal practice concerned, taking all the money she earned and treated the woman as a "human commodity".

Example 3

In November 2019, officers of the Central Investigation Bureau of the Police (CBŚP) and the Border Guard, under the supervision of the National Prosecutor's Office, dismantled an organised criminal group whose members organised the transfer of foreigners to Western European countries. The criminal group operated throughout Europe. Its members organised transfer channels for foreigners starting in Romania, through Poland, to Germany, the United Kingdom and France. Vietnamese citizens paid for such a "trip" from USD 6.5 thousand to USD 20 thousand. As a result of joint actions of the services concerned, 10 people were detained, and earlier the smuggling of 21 foreigners was prevented. The smuggled people were transported from Romania in compartments hidden in the cargo spaces of trucks. These hiding places were specially constructed, placed behind the transported goods, and made it impossible for the foreigners hidden inside them to get out on their own. The transfer of foreigners took place in stages. Poland was a place where smuggled people stayed while waiting for final transport to their destination. According to the findings of the Polish services, 13 people were also detained in Germany and the United Kingdom. The suspects were charged with participating in an organised criminal group that arranged the crossing of the border of the Republic of Poland for foreigners, contrary to applicable regulations. One person was also charged with leading this group.

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

General characteristics

299. Financial gains that are subsequently the subject of the prohibited act specified in Article 299 of the Penal Code may also come from crime related to infringement of copyright and industrial property rights.

300. Articles 115-122 of the *Act of 4 February 1994 on copyright and related rights* (Journal of Laws of 2022, item 2509) contain criminal provisions penalising copyright infringement. Article 115(1) of this Act penalises appropriation of authorship or misleading as to the

authorship of another person's work or artistic performance. Dissemination of another person's work in the original version or in the form of an arrangement, artistic performance, phonogram, videogram or broadcast, or public distortion of such a work, artistic performance, phonogram, videogram or broadcast (Article 115(2)), without specifying the name or pseudonym of its creator, is also punishable. Distributing another person's work in its original version or in the form of an arrangement, artistic performance, phonogram, videogram or broadcast without authorisation or contrary to its terms is also subject to criminal liability (Article 116(1)), so is the recording or reproduction of such a work for the purpose of its dissemination (Article 117(1)). The Act also penalises activities consisting in acquiring, aiding in selling, accepting or aiding in concealing an item carrying a work, artistic performance, phonogram or videogram distributed or reproduced without authorisation or contrary to its terms (Article 118(1)).

Table 15. Police data regarding criminal proceedings conducted in 2019-2021 under the Act on copyright and related rights[124]

Year	Proceedings initiated	Offences ascertained	Offences detected	Detection rate (%)
2021	459	3,279	3,155	96.10
2020	691	11,267	11,034	97.90
2019	1,238	3,703	2,633	71.00

301. The *Act of 30 June 2000 – Industrial Property Law* (Journal of Laws of 2023, item 1170) provides for criminal liability for attributing authorship or misleading another person as to the authorship of someone else's inventive design, as well as violating the rights of the creator of an inventive design in any other way (Article 303). It is also penalised, among others, to apply for a patent with respect to someone else's invention (Article 304). Pursuant to this Act, proceeds subject to laundering as part of the offence stipulated in Article 299 of the Penal Code are, however, generated primarily from trade in goods bearing counterfeit trademarks. Pursuant to Article 305 of the Act, anyone who labels goods with a counterfeit trademark or registered trademark which they are not authorised to use for the purpose of marketing goods bearing such trademarks, or who trades in goods bearing such trademarks, shall be 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)).

Examples of sanitised cases

Example 1

In October 2021, officers from the Department for Combating Economic Crime of the Poviat Police Headquarters in Dzierżoniów, dealing with combating economic crime, completed proceedings regarding the marketing of watches with counterfeit trademarks of well-known manufacturers. This illegal practice took place in 2020. As a result of operational activities and then procedural work, evidence was collected that allowed for bringing charges against a 29-year-old resident of the Dzierżoniów Poviat. The man was involved in the sale of watches via

[124]https://statystyka.policja.pl/st/wybrane-statystyki/wybrane-ustawy-szczegol/ustawa-o-prawie-autorsk/50878,Ustawa-o-prawie-autorskim-i-prawach-pokrewnych.html, access on 21.04.2023

an online store and an auction portal. The police officers seized the watches and ended the illegal activity. The rightful manufacturers estimated the losses at more than PLN 724,000. The suspect was charged with the marketing of goods labelled with a registered trademark that he had no right to use.

Example 2

Police officers from the Department for Combating Economic Crime of the Warsaw Metropolitan Police Headquarters detained a 30-year-old man who was selling leather products bearing counterfeit trademarks of a well-known brand in the Shopping Centre in Wólka Kosowska. As a result of the search of the stand, the police officers seized 768 handbags with counterfeit trademarks. The market value of the seized goods, calculated by the aggrieved companies, was almost PLN 3 million. During the proceedings, it was confirmed that the goods seized by the Police were imported directly from China. The detainee testified that the goods were ordered by the co-owner of the company. The police officers also identified the accounting office responsible for the company's financial settlements, which may help determine the scale of this illegal practice. The detained man will be charged with the marketing of goods illegally labelled with trademarks of famous global brands. This act may meet the criteria of Article 305(3) of the Industrial Property Law Act, i.e. the perpetrator has made this offence a permanent source of income or commits this offence in relation to goods of significant value – in this case he is subject to imprisonment for a period from 6 months to 5 years.

5.1.7. Offences related to the infringement of environmental protection laws

General characteristics

302. Financial gains that are subsequently the subject of the prohibited act specified in Article 299 of the Penal Code may also come from crime related to infringement of environmental protection laws. Any action that infringes environmental protection law and has very harmful effects on the environment or human health or poses a serious threat to the environment or human health may be recognised as an offence against the environment. Nowadays, significant profits are derived, in particular, from crime related to illegal waste management.

Abandoning waste, including hazardous waste, in places not intended for this purpose is currently one of the most serious problems. The responsibility for removing hazardous waste often falls on local government authorities because the perpetrators cannot be identified. The costs of disposal of abandoned waste are a heavy burden for the state and local government budgets – even several dozen million zlotys (e.g. the cost of the removal of illegal waste in Gorlice amounted to almost PLN 49 million)[125]. Hence the significant profits of criminals involved in this illegal practice. The scale of the problem is reflected in approximately 900 such storage places identified by the Chief Inspectorate of Environmental Protection. In recent years, there has been a marked upward trend in the number of fires at waste storage sites. Many of these fires are set in an attempt to conceal an offence. Throughout Poland, there were 75 such fires in 2012, 82 in 2013, 88 in 2014, 126 in 2015, 117 in 2016, 132 in 2017, 243 in 2018 and 177 in 2019. In 2019, the greatest numbers of fires at waste storage sites were recorded in the following voivodeships: Lubuskie (34), Mazowieckie (29) and Lubelskie (25)[126].

[125] https://www.gov.pl/web/sprawiedliwosc/koniec-z-lagodnymi-karami-dla-niszczacych-srodowisko
[126] source: Ochrona środowiska 2020 (Environmental Protection in 2020), GUS, Warsaw, 2020, pp. 161-162

In 2022, the Supreme Audit Office carried out audit proceedings regarding the prevention of fires at waste storage sites The findings of this audit were included in the document entitled "Information on the findings of the audit regarding the prevention of fires at waste storage sites"[127]. It was determined that 754 fires at waste storage sites (including illegal ones) occurred in Poland in 2017–2022. According to Statistics Poland data, as at the end of 2020, there were 2,008 illegal waste storage sites (illegal dumpsites), with a total area of almost 2 km², including 1,111 ones in rural areas and 897 ones in towns and cities. This is not the total number of such sites, because according to the auditors, there may be even more of them. In 2020, mainly plastic and textile waste, as well as alternative fuels and hazardous waste, and in single cases also car wrecks, waste electrical and electronic equipment, bulky waste, municipal waste and paper and cardboard burned at waste storage sites.

Fires at waste storage sites may be often associating with committing an offence (e.g. intentional or accidental arson, self-ignition of waste due to negligence or faulty security measures), which requires the initiation of investigative proceedings by the Police and a prosecutor's investigation.

Table 16. *Number o*f identified and detected offences related to a dangerous incident *in the form of a fire in 2017-2020 (data from the Police Headquarters)*

Offences under Article 163(1)(1) of the Penal Code	**2017**	**2018**	**2019**	**2020**
Ascertained	239	259	314	64
Detected	84	97	103	34

303. The number of offences against the environment has been increasing in recent years. According to data from the Police Headquarters, this increase is especially visible in the case of offences under Article 183 of the Penal Code, i.e. illegal waste management. In 2020, 287 such offences were committed, compared to only 28 ones detected in 2017, which represents an almost 10-fold increase in a few years. Article 183 of the Penal Code penalises, among others, illegal storage, removal, processing, recovery, disposal and transport of waste which may threaten human life or health or cause significant degradation of water, air, land surface or losses in plants or animals (Article 183(1) of the Penal Code). The Penal Code provides for a penalty of imprisonment for a period from 3 months to 5 years for the act described above. It also penalises imports and exports of hazardous waste without the required notification or permit or contrary to the terms and conditions contained therein. This offence is punishable by imprisonment for a period from 6 months to 8 years (Article 183(5) of the Penal Code).

304. The main cause of offences related to illegal trade in and storage of waste are the high costs of waste disposal in the European Union. Illegal trade in waste may also be used to legalise profits generated through other criminal activities. Offences related to illegal waste trade and storage are accompanied by forging transport documents, making it impossible to determine the actual waste collection site. Agreements with owners/users of real estate where waste is to be stored are concluded using forged documents, for shell companies that do not conduct actual business activities in order to transfer the costs of waste disposal to these entities and make it difficult to determine the actual origin of this waste. Funds originating from illegal activities

[127] https://www.nik.gov.pl/aktualnosci/zapobieganie-pozarom-miejsc-gromadzenia-odpadow.html, access on 24.04.2023

are most often deposited using a fictitious account set up to carry out one or several transactions, using the greatest possible number of fictitious elements, e.g. forged documents or providing a false purpose for opening an account or an ultimate account, set up to transfer funds, from which these funds are immediately withdrawn in cash.

Table 17. Police statistical data[128] *–waste mismanagement (Article 183 of the Penal Code), 2017-2020*

Waste mismanagement (Article 183 of the Penal Code)			
Year	**Number of proceedings initiated**	**Number of offences ascertained**	**Number of offences detected**
2020	454	352	287
2019	412	167	109
2018	345	94	70
2017	249	51	28

Examples of sanitised cases

Example 1

From May 2019, police officers from the Criminal Department of the Voivodeship Police Headquarters in Katowice were investigating the case of the so-called garbage mafia. As a result, the Police dismantled two organised criminal groups, the prosecutor brought charges against 27 individuals, and the suspects' cash and other assets worth almost PLN 3.5 million were seized. The investigation began in February 2019 in Żory. 14 truck semi-trailers filled with tanks with an unknown substance were discovered on private real estate. Mauser containers with a capacity of 1,000 litres each and 200-litre barrels were placed on the semi-trailers. In total, the tanks contained approximately 700,000 litres of substance. The truck semi-trailers, that were in very poor technical condition, were used as warehouses for illegal waste storage and abandonment.

As a result of many months of investigation, the Police smashed two organised criminal groups involved in illegal storage of hazardous waste. It was established that these groups operated in various places in the Śląskie Voivodeship, as well as in the southern and central parts of Poland. The waste disposal methods varied. The criminals rented warehouses or fenced areas. Then they filled the warehouses with containers with liquid waste, and in open areas, they placed semi-trailers filled with tanks with waste. Once the warehouses and trailers were filled, the criminals disappeared. The criminal groups also buried containers and barrels with waste in the ground, and even emptied them pouring the waste directly onto the ground or in forest. In this way, they abandoned a total of approx. 14.5 thousand tonnes of waste. The Police established that the first of the dismantled criminal groups carried out their illegal activities from 2015 to September 2019. The other group operated from 2018 to February 2019. All suspects were charged with participating in an organised criminal group, threatening the lives or health of many people, and transporting and storing waste contrary to the provisions of the Act. Two suspects were also charged with leading a criminal group. The Police also found that in some cases, the warehouse owners were aware that criminals would illegally store waste on the rented premises, for which they were charged as well. The Police also seized property (cash,

[128]https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-3/63476,Nieodpowiednie-postepowanie-z-odpadami-art-183.html

immovable and movable property, including vehicles owned by the suspects) with a total value of almost PLN 3.5 million.

Example 2

In April 2019, officers from the Voivodeship Police Headquarters in Katowice dealing with combating economic crime detained members of an organised criminal group involved in illegal trade in harmful waste threatening the lives and health of many people. As established in the investigation conducted under the supervision of the Regional Prosecutor's Office in Katowice, the criminals would rent warehouse halls in various location throughout Poland (including Częstochowa and Zawiercie). The criminals concluded contracts for companies registered in their name or in the name of third parties – family members or straw men. Then they illegally stored waste on the rented premises. This was liquid waste, including derivatives of solvents and varnishes, as confirmed by experts in the field of physical chemistry. Waste was usually stored in 1,000-litre mauser containers and in 200-litre barrels. Once the area was filled with waste, the perpetrators abandoned it in conditions that could pose a threat to human life or health or could cause environmental contamination. On each of the rented premises, the criminals usually left even several thousand tanks filled with hazardous liquids and disappeared, leaving the owners of the land or warehouses in quite a predicament. The criminal activity involved transport companies whose owners, despite of being aware of possible criminal liability, established cooperation with the head of the "waste" mafia, as well as individuals whose role was to falsify transport documentation, search for appropriate places to store dangerous chemicals and individuals who concluded warehouse lease agreements using fictitious data. The suspects were charged with participating in an organised criminal group, money laundering, as well as transporting and storing waste contrary to legal regulations.

5.1.8. Other predicate offences

305. Other types of predicate offences include offences committed on the financial market (i.e. stock exchange offences, insurance offences, conducting business without a licence), offences related to illegal gambling, and offences against the credibility of documents.

306. *The Act of 29 July 2005 on trading in financial instruments* regulates, among others, the principles, procedure and conditions for undertaking and conducting business consisting in trading in financial instruments. It also provides for criminal liability for offences involving: illegal conduct of business consisting in 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 secrecy or official secrecy (Article 179), disclosure or use of inside information (Article 180), recommending or inducing others to buy or sell financial instruments to which inside information relates (Article 182), manipulating financial instruments (Article 183(1)), and entering into an agreement aimed at manipulation (Article 183(2)). These offences may lead to obtaining financial gains subject to laundering.

307. Penal provisions are also included in the *Act of 27 May 2004 on investment funds and the management of alternative investment funds*. As far as generating illegal profits subject to subsequent laundering is concerned, the most significant offences are covered by Articles 287

and 289 of the aforementioned Act. The first of the aforementioned articles provides for criminal liability for conducting, without the required permit or contrary to 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 shall be imposed on a person who, being obliged to observe professional secrecy, discloses it or uses it contrary to its intended purpose. Where the offender acts to obtain a financial or personal advantage, they are subject to stricter criminal liability.

308. 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 a regulated market are governed 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)[129]. It also defines the obligations of issuers of securities and other entities involved in trading in these 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, imprisonment for up to 2 years, or both (Article 99). Criminal liability shall also be imposed on a person responsible for the information contained in the prospectus or other information documents or for other information related to the public offering or admission or application for admission of securities or other financial instruments to trading on a regulated market, who provides false data or conceals true data, materially affecting the content of the information. In the case of such offences, the perpetrator usually seeks to achieve a personal or financial advantage.

309. The Polish Financial Supervision Authority (KNF) plays an important role in disclosing this type of offences. Pursuant to Article 6b(1) of the *Act of 21 July 2006 on the financial market supervision*, this authority shall make public information on its notifications of suspected offences specified in the following provisions:

- Articles 215 and 216 of the *Act of 28 August 1977 on the organisation and operation of pension funds*,
- Article 171(1)-(3) of the *Act of 29 August 1997 – Banking Law*,
- Articles 56a and 57 of the *Act of 26 October 2000 on commodity exchanges*,
- Article 430 of the *Act of 11 September 2015 on insurance and reinsurance activities* (before 1 January 2016 – Article 225 of the *Act on insurance activities*),
- Articles 47 and 48 of the *Act of 22 May 2003 on insurance brokerage* (Journal of Laws of 2023, item 1111),

[129] 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 (OJ L 168, 30.06.2017, p. 12), that largely modifies the provisions of the aforementioned Act, will apply in this regard.

- Article 50(1) and (2) of the *Act of 20 April 2004 on employee pension schemes* (Journal of Laws of 2023, item 710),
- Article 40 of the *Act of 20 April 2004 on individual retirement accounts and individual retirement security accounts* (Journal of Laws of 2022, item 1792)
- Article 287 and Articles 290-296 of *Act of 27 May 2004 on investment funds and the management of alternative investment funds*,
- Article 178 of the *Act of 29 July 2005 on trading in financial instruments*,
- Articles 99 and 99a of the *Act of 29 July 2005 on public offering, conditions governing the introduction of financial instruments to organised trading, and public companies*,
- Articles 150 and 151 of the *Act of 19 August 2011 on payment services*.

310. In 2021, the Office of the Polish Financial Supervision Authority (UKNF) sent 98 notifications[130] on suspicion of committing an offence to the National Prosecutor's Office, the Circuit Prosecutor's Office in Warsaw, the Regional Prosecutor's Office in Warsaw and District Prosecutor's Offices, relating to 135 violations of criminal law provisions. In 2021, 40 letters supplementing the submitted notifications were also sent to prosecutor's offices.

311. Pursuant to Article 6b(6) of the *Act of 21 July 2006 on the financial market supervision*, the KNF also notifies of criminal proceedings conducted *ex officio* or as a result of a notification submitted by an entity other than the KNF, where the Chairperson of the KNF exercised the rights of the injured party in criminal proceedings.

312. Business activity involving gambling is regulated in Poland by the *Act of 19 November 2009 on gambling*. Pursuant to Article 3 of the aforementioned Act, organising games of chance, betting, card games and games on gaming machines, as well as conducting business activity in this field, is permitted under an appropriate licence, permit or notification. Illegal gambling is often a source of considerable income for criminals, that is subsequently laundered.

313. As regards crime related to the operation of the gambling market, a number of different ways of violating legal provisions are reported by the Police, describing the methods of operation of criminals, especially via the Internet. Unlimited access to the Internet worldwide creates the potential for circumventing Polish regulations and transfers illegal gambling to cyberspace. As far as money laundering is concerned, the Police identify several *modus operandi*, including:

- online casinos allow money transfers directly between customers without passing through a casino account – customers can therefore borrow funds from unconventional sources (risk of money originating from illegal activities),
- many e-wallets accept cash as deposits – the customer makes a deposit to the e-wallet using the account of a financial institution; the confirmation issued by this institution

[130] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku (Report on the activities of the Office of the Polish Financial Supervision Authority and the Polish Financial Supervision Authority in 2021), Warsaw, 2022, p. 187 and at: https://www.knf.gov.pl/publikacje_i_opracowania

will only include the deposit to the e-wallet, not the transaction with the online casino,

- online poker games often take place on platforms that are shared by multiple casino operators – the platform plays a key role in monitoring the pattern and value of the game in terms of potential money laundering activities, for example chip dumping,
- a growing popularity of online gambling games in which the criminal deposits funds into an appropriate account linked to the gambling platform is recorded. The funds are transferred back to the platform customer in the form winnings, which makes it easy to conceal the player's identification details, especially in the case of foreign online casinos.

314. Pursuant to Article 107(1) of the Penal Fiscal Code, anyone who, contrary to the provisions of the Act or the terms of the licence or permit, arranges or conducts gambling games, shall be held liable under the aforementioned provision. Committing this prohibited act in order to obtain financial benefits from organising collective participation in a gambling game shall be subject to stricter criminal liability (Article 107(3) of the *Penal Fiscal Code*).

315. The *Penal Fiscal Code* also penalises selling lottery coupons or other evidence of participation in a game of chance, betting or a game on gaming machines in order to achieve financial gain without being authorised to do so (Article 110 of the *Penal Fiscal Code*).

316. According to the Police information, in 2019, the CBŚP initiated 1 preparatory proceeding regarding irregularities related to gambling, while 10 such proceedings were pending. The value of losses related to the activities of criminal groups dealing with this form of crime amounts to PLN 21.4 million. In 2019, 18 individuals were charged in cases regarding gambling offences, including 1 under Article 258 of the *Penal Code*, and 20 under Article 299 of the *Penal Code*. Property worth PLN 4 million was also seized, while the amount of laundered money in these cases was PLN 38.5 million. In 2020, the CBŚP was conducting 6 preparatory proceeding regarding irregularities related to gambling. The value of losses related to the activities of the criminal groups involved in these offences was PLN 270 million. Charges in cases regarding gambling offences were brought against 78 individuals, including 39 under Article 258 of the *Penal Code* and 12 under Article 299 of the *Penal Code*. Property worth PLN 8.6 million was also seized, while the amount of laundered money in these cases was PLN 138.8 million.

Examples of sanitised cases

Example 1
In mid-2021, officers of the Silesia Branch of the National Revenue Administration (KAS), the Internal Inspection Office of the Ministry of Finance and police officers from the Voivodeship Police Headquarters in Katowice dismantled two organised criminal groups that were involved in illegal gambling in Silesia. Gang members were detained and arcades with illegal gambling machines were closed down. The investigation is being conducted by the Silesia Branch of the

Department for Organised Crime and Corruption of the National Prosecutor's Office in Katowice. The services began cooperation in connection with information about the activities of two criminal groups that organised illegal gambling games. Officers of the Customs and Tax-Control Service were suspected to be involved in these illegal activities. As a result of the operational activities carried out on 15 June 2021, several hundred police officers and officers from the Ministry of Finance and the KAS from Silesia, Lesser Poland and Masovia entered the flats of members of the criminal groups and premises where illegal gaming machines were located. The activities were carried out simultaneously in many poviats. A total of 38 arcades where illegal gambling games were organised were closed down. The officers seized 209 illegal slot machines, a roulette, almost PLN 1.5 million in cash (in various currencies) and a luxury car. Over PLN 0.5 million and material evidence was seized from the Customs and Tax-Control Service officers faced with imprisonment of up to 15 years. Evidence proving that they were corrupted was also obtained. The well-organised criminal groups had been operating since 2018. As a result, 2 criminal groups were dismantled, their 17 members aged 25-46, including the 34-year-old leader of one of the gangs, and 4 officers of the Customs and Tax-Control Service were detained. All of them are residents of the Śląskie Voivodeship. The groups had been organising illegal gambling since January 2018. Their structure was hierarchical, with a permanent division of tasks and roles in each group. The court arrested 15 suspects, while 2 suspects have been covered with police surveillance imposed by the prosecutor. The group leader faces imprisonment of up to 15 years, while the other members may be sentenced to 10 years in prison.

317. As for offences against the credibility of documents, the number of such cases ascertained in 2020 was relatively large and accounted for approx. 7.0% of all ascertained offences. These were offences penalised in Articles 270-277 of the Penal Code.

318. Since 12 July 2019, the provisions of the *Act of 22 November 2018 on public documents* (Journal of Laws of 2023, item 1006) have been in force, including its Article 58 that reads as follows: "Whoever produces, offers or sells a replica of a public document or stores such a replica for it to be sold shall be subject to a fine, restriction of liberty or imprisonment for up to 2 years."

319. In connection with the hostilities on the territory of Ukraine, the Polish Police identifies new *modi operandi* as regards predicate offences for money laundering. These concern offences related to organising aid/fund-raisers for Ukrainian citizens in connection with the war. Russia's aggression of Ukraine started on 24 February 2022 resulted in many initiatives in Poland and around the world aimed at providing aid to Ukrainian citizens harmed by war operations. This activity includes, among others, organising online fund-raisers. This increases the risk of such activities being conducted by unverified entities with a vague ownership structure. Offenders use emotional content to encourage potential donors to donate money. Attempts have also been identified to encourage donors to purchase newly created cryptocurrencies or special tokens, whereby there is no guarantee that the donated funds will reach those in need. Moreover, due to the migration of a significant number of refugees to Poland, there is an increased risk of fraud using personal data obtained illegally.

5.2. ESTIMATES OF PROCEEDS OF CRIME SUBJECT TO LAUNDERING

320. Assets subject to laundering generally originate from hidden or even illegal activities. In practice, this means that it is impossible to directly observe and determine the scale of this practice. Money laundering is necessary for carrying out criminal activities or participating in the unofficial economy, or even a condition for the existence of such phenomena. This is particularly noticeable in the case of funds derived directly from crime. The European Union recognises organised crime as one of the greatest threats to the security of the Community. In 2019, the European Council estimated revenue from major criminal activities at EUR 139 billion, which represented 1% of the total EU GDP[131]. At the same time, it is indicated that the EU is moderately successful in recovering assets originating from crime. It is estimated that only 2% of funds originating from crime are recovered from criminals[132]. Profits from illegal activities are estimated using the SOCTA methodology, focused on five key areas related to the activities of criminal organisations. EUROPOL collects data on criminal groups and those involved in them, areas of operation of serious criminals and organised crime, the impact of committed offences, the infrastructure used by perpetrators and the environment in which criminal activities take place. Qualitative and quantitative methods are used in the data evaluation process. The data is provided by EUROPOL member states, and the indicators developed based on this data are positioned in accordance with the weights assigned by the SOCTA Advisory Group[133].

321. The estimation of profits from strictly criminal activities that are particularly concealed by the perpetrators is a major problem. It cannot be assumed that any assessment of these activities corresponds to their actual size. All data obtained is assumptions and estimates.

322. Eurostat attempted to develop a method for estimating profits from criminal activities in "Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments"[134]. For the purposes of that study, it was assumed that illegal activities include transactions that are forbidden by law and transactions that are not illegal *per se* but become illegal if carried out by unauthorised persons[135]. The document clearly distinguishes illegal transactions and other transactions carried out in the non-observed economy, e.g. production carried out by households for their own final use. In this case, the document refers to the UN System of National Accounts 2008 that states that there are two types of illegal production, i.e.:

- the production of goods or services whose sale, distribution or possession is forbidden by law;
- production activities that are usually legal but become illegal when carried out by unauthorised producers[136].

---

[131] The EU's fight against organised crime - Consilium (europa.eu), access on: 24.06.2022
[132] Shadow money - the international networks of illicit finance. The law enforcement perspective in the wake of the Pandora Papers Leak. Europol Spotlight series, 2021 ., p. 14.
[133] EU SOCTA 2021. Serious and organized crime threat *assessment. A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime.* Europol, 2021, pp. 100-104.
[134] Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments, Eurostat, 2018,
[135] Handbook on the compilation …, p. 17
[136] UN System of national Accounts 2008, p. 100

Thus the Eurostat document repeats the definition adopted by the UN.

323. The EU organisation notes that including profits from illegal activities in macroeconomic data is necessary due to the need to reflect the full picture of the economy of a given country, which is undoubtedly influenced by the illegal sector. For this purpose, EUROSTAT has prepared methodological guidelines for estimating the level of profits from criminal activities. A division has also been made into transactions that require the conscious participation of two parties, e.g. the purchase of narcotic drugs, and other offences where either of the parties are not willing participants, e.g. theft or fraud.

324. The methodology has been developed for three types of offences identified as the most economically material (generating the highest profits) and involving conscious transactions:

(1) Prostitution. The study notes that assessing the profits from this type of activity is difficult due to the fact that certain types of prostitution are legal in many countries of the Community. Eurostat notes that in all countries, at least some data regarding this segment are available, but in most cases, these are *ad hoc* studies on the subject or irregular reports by police. Demand side studies are not sufficient to estimate the phenomenon in question. As a starting point, it was recommended to estimate the number of prostitutes in a given country, broken down by different types of prostitution service, differentiating further (in some countries) between legal and illegal prostitution. For each type of prostitution, the average number of contacts per prostitute per period should be estimated in order to produce the total number of contacts. With this information and data on service prices, it is possible to calculate the value of transactions for specific types of prostitution and the total value of transactions. It may also be assessed whether the services are provided by residents or non-residents. In this case, an assessment is necessary to determine whether the calculated transaction value is a component of domestic output or import of services. It is also necessary to determine the level of consumption separately for each type of prostitution, as there are types of sexual services that are never legal, e.g. prostitution of minors or forced prostitution. Regardless of a given country's attitude towards this phenomenon, illegal categories of prostitution and sexual services are subject to a separate assessment related to the need to combat such practices. The level of expenses accompanying sexual services, including the cost of renting premises where these services are rendered, purchase of alcohol, etc. may also be assessed[137];

(2) Production and trafficking of drugs. The aforementioned activities are considered illegal in all countries of the European Union and the European Free Trade Association. Cannabis, ecstasy, amphetamine, cocaine and heroin are considered illegal in all countries. Some countries add LSD and other hallucinogens as well as illegally used medical substances to this list. The study indicates that due to the hidden nature of this phenomenon, estimates have to rely on the following sources: (I) data provided by administration bodies, the Police, customs services, etc., (II) data obtained by the health service and institutions established to combat drug consumption, (III) expert research, (IV) data collected by non-profit organisations, (V) international research projects. The study indicates that the assessment process should start with estimating the level of

[137] Handbook on the compilation…, par. 3.4.

domestic drug consumption, broken down by drug type, consumer category, etc. The consumer category is important due to the fact that regular (addictive) users consume different amounts and types of prohibited substances and with a different frequency than occasional users, thus affecting the overall consumption level in a different way than the latter. The amount of expenses is subsequently determined based on the average retail price data. When determining the quantity of drugs placed on the market, their purity should be taken into account, due to the fact that a significant part of drugs in retail trade is diluted (mixed) with substances that increase their weight. Finally, after estimating the quantity of drugs being traded and their value, the suppliers' margin and their final profit can be calculated. To calculate the profit, it is necessary to determine the costs of production and transport of drugs, relying on expert estimates[138];

(3) Smuggling of alcohol and tobacco products. Eurostat clearly distinguishes between smuggled goods and illegal production within a given country, noting that smuggling most often concerns goods that are legally traded in a given country, that for some reason are not available in the adequate quantity or at an affordable price. In the case of alcohol and tobacco products, the competitiveness of illegal transport thereof is most often due to the tax burden. According to Eurostat guidelines the price of smuggled goods can be determined based on wholesale prices in a given country. However, Eurostat does not specify how to estimate the quantity of smuggled goods. It has been assumed that these products are sold directly to households, bypassing official sales channels. To calculate the final margin and the smuggler's profit, it is necessary to determine the unit price in retail sales, which can also be done based on expert estimates. Expert estimates are also used to determine the costs incurred while smuggling the goods[139].

325. "Handbook on the compilation..." also provides for the methodology for other types of criminal transactions, covering less economically material offences. These concern activities (I) where both parties are willing participants, (II) that are legal *per se*, but are hidden in order to bypass the official procedures related to them, (III) that are performed informally, without officially documenting them.

The Eurostat document lists the following types of observed offences:

(1) illicit firearms trafficking;

(2) fencing of stolen goods;

(3) migrant smuggling;

(4) infringement of intellectual property rights;

(5) bribery;

(6) illegal gambling;

(7) money laundering[140].

[138] Handbook on the compilation…, par. 3.5.
[139] Handbook on the compilation…, par. 3.6.
[140] Handbook on the compilation…, par. 4.

326. As in the case of other types of activity, the perpetrator's profit is the value of sales made less costs. The Handbook indicates that in the absence of direct data on this type of activity, it is necessary to rely on all available data, such as police statistics, data collected by government and non-governmental organisations, etc. However, this data documents only a small part of the illegal transactions disclosed. There is no direct data on the output of illegal goods and the actual costs of committed offences. According to the Handbook there is no single fully reliable method to estimate profits from crime. Each subsequent method introduces the risk of statistical error due to incomplete input data, limited amount of source materials, observations that do not fully reflect reality, etc. The value of profits from committed offences can only be estimated based on the adopted assumptions, whereby the data used for the estimates includes only those criminal transactions that have been disclosed. Analyses should always account for the existence of undisclosed numbers of illegal profits and their underestimation.

327. In the case of offences that do not involve transactions, including theft, fraud, etc., it can be assumed that the thus obtained proceeds approximate the amounts provided by the victims when reporting the offence. However, also in this case it must be assumed that not all offences are reported. This method also involves risk where material goods whose value was not clearly determined have been lost. There may be a mistake resulting in an underestimation or overestimation of the value of, for example, a stolen item. It is also difficult to clearly determine the profit of a potential criminal because there is no information about the possible costs of their activities. However, for this category of crime, official statistics seem to be the best source of data.

328. It should be noted that profits from crime constitute part of the non-observed economy, i.e. shadow economy. From the point of view of economic life, the shadow economy brings numerous negative effects through creating distorted economic statistics, depleting tax revenue and social insurance premiums, increasing the risk of debt, improper disposal of social benefits, increasing fiscal burdens, distorting competition rules, reducing the level of employee protection. etc.[141]. Assessing the scale of this phenomenon is therefore crucial. Much information in this area is provided in Prof. Friedrich Schneider's research conducted at the University of Linz. To assess the size of the shadow economy in various countries around the world, he uses the MIMIC economic model that takes into account:

- monetary indicators regarding financial flows necessary for the shadow economy to operate,
- labour market indicators, observing such circumstances as potential employee flows between the shadow economy and the official economy or observed working hours,
- production market indicators examining relationships in the official economy that may indicate a growth of the unofficial sector.

329. Due to the wide scope of research conducted by Professor Schneider, his results are often cited in attempts to assess the shadow economy. It should be noted that in the case of European Union countries, they are usually 1/3 higher than official estimates.

[141] M. Pasternak-Malicka, Pozytywne i negatywne konsekwencje szarej strefy postrzeganej jako "zręczność podatkowa" podmiotów gospodarczych i gospodarstw domowych, Zeszyty Naukowe SGGW, Polityki Europejskie, Finanse i Marketing, 24(73), pp. 131-133.

330. Due to the processes triggered by the COVID-19 pandemic, Schneider forecasts an increase in the size of the shadow economy in the countries he examines. This phenomenon led to a severe recession in the affected countries, resulting in a decline in employment and a sharp decline in GDP[142]. For Poland, an increase in the share of the shadow economy is forecast for 2020 and 2021, to 22.45% and 22.02%, respectively, In 2022, this share is to be 21.89%, with the average for EU countries of 17.29%[143].

331. Determining what the shadow economy actually is a challenge for researchers. The very nomenclature varies, including terms such as unofficial economy, unregistered economy, hidden economy, etc. Various definitions of this phenomenon are provided, but most often the unofficial economy is considered to be an economic activity that creates added value, but is not subject to registration in the national account. Some researchers exclude in this respect production carried out by households for own final use[144]. However, the essential feature is to avoid situations in which a given activity would be officially observed or taxed.

332. In fact, not every unregistered activity is related to criminal activity. Most studies note the division of activities in this sector. The distinction concerns:

- strictly illegal activities related to crime, i.e. committing a prohibited act under penalty provided for in the applicable law specifying its characteristics, that is culpable and socially harmful to a degree higher than negligible[145],
- manufacturing or service activities that are legal *per se*, but become illegal when performed in a hidden manner, circumventing procedures provided for in labour law, tax law and other provisions applicable to this activity.

333. Not every activity is considered a crime due to the lack of a relevant legal standard prohibiting a given act, the degree of social harmfulness, culpability, etc. Undoubtedly, it is one thing, for example, where a given person makes a profit from trafficking drugs, and another thing if the same person makes a living by doing odd jobs off the books. Therefore, the black and shadow economies must not be clearly equated and revenue obtained from such sources must not be treated in the same way.

334. Statistics Poland has adopted the definitions of the phenomena in question recommended by the OECD and Eurostat, according to which[146]:

(1) An unobserved economy is an area of the economy that includes a group of economic activities that are most likely to be unobserved. These are:

(a) underground production;

(b) illegal production;

[142] F. Schneider, New COVID-related results for estimating the shadow economy in the global economy in 2021 and 2022, International Economics and Economic Policy volume 19 (2022), p. 302.
[143] F. Schneider, New COVID-related results…, p. 303 and p. 307.
[144] M. Masternak-Malicka, Szara strefa – definicje, przyczyny, szacunki. Polska perspektywa zjawiska; Studia BAS, Nr 2 (58) 2019, p 30.
[145] Article 1 of the Act of 6 June 1977 – Penal Code (consolidated text: Journal of Laws of 2022, item 1138).
[146] Measuring the Non-Observed Economy. A Handbook OECD, 2004, pp. 13-14

(c) informal sector production or production of households for own final use. An activity may also be omitted due to deficiencies in the way basic statistical data is collected;

(2) Underground production includes production activities in the economic sense, that are completely legal (in terms of meeting standards and legal regulations), but hidden from public authorities to:

(a) avoid paying due taxes;

(b) avoid paying social insurance premiums;

(c) avoid the application of legal requirements such as minimum wage, maximum working hours, work safety conditions;

(d) avoid administrative procedures such as completing statistical questionnaires and other forms;

(3) Illegal production includes:

(a) production of goods and services whose sale, distribution or possession is prohibited by law;

(b) to a lesser extent, production activities that are legal *per se*, but become illegal when carried out by unauthorised producers, for example, providing health care services without a licence or manufacturing a legal product that does not meet prescribed technical standards.

335. The above should also take into account national specifics, e.g. prostitution – that is legal in some countries while it is illegal in others. Polish solutions provide for a distinction into the services of sex workers, being part of the unofficial economy, and pimping and profiting from prostitution, which is illegal.

336. Studies point to numerous threats that may result in the expansion of underground production in the economy. The introduced lockdowns resulted in shutting down some parts of the economy and limiting access to some services. Measures to counteract the spread of the disease reduced the scope of the official economy. Some entities operating in these industries began to conduct their activities unofficially. A significant number of employees of entities closed during the pandemic found unregistered employment. The spending of public funds intended to combat the virus increased the risk of corruption and abuse in their spending. The COVID-19 pandemic also caused an increased threat of greater demand for narcotic substances. According to the UNODC World Drug Report 2021, the pandemic has pushed over 100 million people into extreme poverty, led to the loss of 255 million jobs worldwide, and caused an increase in the incidence of mental health disorders. These factors may increase the demand for drugs. The pandemic is also changing the operation of the drug market: the consumption of cocaine and various forms of MDMA (ecstasy) has decreased, and the consumption of cannabis has increased significantly. The consumption of sedatives and psychotropic substances used for non-medical purposes is also increasing. The drug market has also changed, as much of it has

moved to the dark web. The value of the global illegal online sales was estimated at USD 315 million annually[147].

337. According to the Shadow Economy 2022 report developed by the Institute of Economic Forecasting and Analysis, the progressive decline in the share of underground production in the Polish economy ceased after the outbreak of the COVID-19 pandemic. A sharp decline in consumption and a long-term administrative freeze on the activities of some industries have reduced the profitability of running a business. Income earned by part of the population has also decreased. Controls carried out by the authorities combined with the still existing demand for certain services (hoteling, restaurants) have redirected some activities and purchasing decisions to the shadow economy. Reduced social mobility and the increased level of non-cash transactions, limiting part of the shadow economy, do not seem to compensate for the negative trends. The situation is even worse due to the ongoing conflict in Ukraine and related changes in Poland's social and economic environment. There is a likelihood of economic slowdown due to recognising Poland as a country directly threatened by the expansion of military operations, significant changes in trade routes, disruptions in financial markets, etc. The influx of a considerable number of refugees and the simultaneous return of some Ukrainian economic migrants back to their country caused changes on the labour market. If adverse developments occur and the conflict continues, the share of the shadow economy may increase to 19.4% of GDP[148]. Therefore, it is particularly reasonable to assess the value of money and property originating from the shadow economy, especially given the fact that significant part of it comes from crime.

338. The GDP value is the key measure of the production volume and changes, describing the size of the shadow economy[149]. Regardless of the research method adopted, the value of the phenomenon concerned is expressed as a percentage of GDP.

339. The shadow economy is an undocumented phenomenon, remaining beyond any possible actual observation. Moreover, it includes not only unregistered activities that are legal *per se*, but also illegal activities prohibited by law, e.g. smuggling, drug trafficking, profiting from prostitution, etc. Such activities are generally hidden. Therefore, any possible attempts to quantify this phenomenon can only be estimates.

340. In 2014, Poland adopted the ESA2010 methodology standard. Since then, Statistics Poland, as the entity responsible for collecting and publishing data, has been obliged to include the value of the unregistered economy in GDP estimates. However, quantifying the amount of income from hidden sources poses significant technical difficulties, mainly due insufficient data and the need to use estimates that Statistics Poland does not make itself. As a result, data prepared by other institutions, statistical data, opinions of expert institutions and research centres as well as statistics of authorised services, e.g. the Police, are used[150].

[147] World Drug Report 2021, United Nations Office on Drugs and Crime, 2021, p. 3.
[148] J. Fundowicz, K. Łapiński, B. Wyżnikiewicz, D. Wyżnikiewicz, Szara Strefa 2022, p. 6.
[149] Anna Czapkiewicz , Katarzyna Brzozowska-Rup, Szacowanie rozmiarów szarej strefy w Polsce, Wiadomości Statystyczne 2021 r., 66(4), p. 12.
[150] Działalność nielegalna w Polsce – założenia metodyczne i wyniki szacunku. Załącznik nr 1 do: Wdrożenie Europejskiego Systemu Rachunków Narodowych i Regionalnych w Unii Europejskiej (ESA2010) do polskich rachunków narodowych, GUS 2014, p. 14.

341. In the *National accounts by institutional sectors in 2016–2019* report prepared by Statistics Poland, it was indicated that the direct method was used to estimate the underground production carried out by legally registered entities. The study covered businesses employing up to 9 people, and public sector entities other than cooperatives, employing from 10 to 49 people. Based on the provided data, standards for the average productivity and average remuneration were established. These were used to estimate global production, intermediate consumption and value added.

342. In the study of unregistered labour, data collected by Statistics Poland in the course of the modular study of unregistered labour as well as the representative study of economic activity of the population conducted by the Department of Demographic Research and the Department of the Labour Market was used. Together with data from official statistics on wages, the numbers of the employed and registered unemployed people were used to estimate the size of the economy in terms of the activity of natural persons performing unregistered work.

343. The estimation of output and the cost of its production by natural persons performing unregistered work was made based on the aforementioned study of businesses employing up to 9 people. The value of aggregate output in this approach is the product of the estimated number of the employed, average remuneration and the ratio of remuneration to aggregate output for small registered entities. The cost of producing this output (intermediate consumption) was calculated using the ratio of intermediate consumption to aggregate output in small registered entities[151].

344. It is particularly difficult to estimate the profits from illegal activities, as they are particularly thoroughly masked. It is often difficult to distinguish between the types of unregistered economy. In each of its segments, there are types of entities similar to legal ones, that make unregistered or illegal transactions for the benefit of informal criminal groups[152]. It is assumed that illegal activity in which one of the parties is not a voluntary participant is not an economic transaction and does not bring added value. Therefore, the shadow economy phenomenon may occur in any area of the economy.

345. The official statistics of Statistics Poland distinguish added value from:

- Prostitution, which is estimated in terms of income earned by sex workers (a shadow economy in the Polish legal system), and pimping involving profiting from the prostitution of other people (considered illegal activity). Calculations are made in accordance with the recommendations of the European Commission (Eurostat), i.e. from supply side approach, separately for three types of prostitution – clubs activity, individuals working on private premises (owned or rented) and street prostitutes. The estimate is a product of the number of persons providing sexual services, number of contacts within the year and the average price of services;
- Trade in narcotic substances. The estimation is made based on data obtained by institutions responsible for combating the phenomenon concerned, including the Police, Customs Service, etc. Data prepared by institutions investigating the phenomenon, e.g. the Office for the Prevention of Drug Addiction and the Institute

[151] Aneks 3. Szara gospodarka i działalność nielegalna w rachunkach Narodowych. Rachunki narodowe według sektorów instytucjonalnych w latach 2016–2019, GUS, July 2021, p. 98,
[152] J. Fundowicz, K. Łapiński, B. Wyżnikiewicz, D. Wyżnikiewicz, *Szara Strefa 2022*, p. 7,

of Psychiatry and Neurology in Warsaw that collects data on consumed amounts and unit prices, is also used. The estimates cover the basic groups of drugs and, in accordance with Eurostat's recommendations, the analysis and estimates of the value of revenue from activities related to the production of and trade in drugs are made from the supply and demand sides. The estimates refer to the major groups of drugs, taking the methods of production, trade and use specific to a given group into account. The estimation takes into account the number of individuals who use drugs occasionally and those who use them regularly, the frequency of use as well as the doses and prices of particular drugs;

- Cigarette smuggling. The demand side (consumption) approach recommended by Eurostat was used to estimate the value of cigarette smuggling in Poland. The estimates are based on numerous data regarding production, sales, consumption, wholesale and retail prices, etc. Both cigarette smuggling from outside the European Union and illegal production in Poland are analysed. The estimates covered each of these cases, whereby the portion of the income related to legally produced cigarettes was included in the shadow economy, while the portion resulting from illegal production and smuggling onto the Polish market was included in the illegal economy. The data comes from institutions dealing with counteracting the phenomenon concerned and from reports on consumer behaviours.

346. According to Statistics Poland estimates, illegal activity constitutes the smallest part of the unobserved economy. Its share in 2016–2019 was stable and amounted to 0.4% of GDP [153].

347. For 2016-2019, Statistics Poland provides the following estimates of the size of the shadow economy and illegal activities in generating GDP[154] (table below):

Table 18. Estimates of the size of the shadow economy and illegal activities in generating GDP in 2016-2019

GROSS DOMESTIC PRODUCT (including unobserved production, in PLN million)	**2016**	**2017**	**2018**	**2019**
	1,863,487.00	1,989,835.00	2,121,555.00	2,293,199.00
	in percentage			
	100	100	100	100
Total non-observed economy	13.3	12.5	12.1	11.1
Shadow economy	12.9	12.1	11.7	10.7
- in registered entities	10.8	10.2	10	9
- attributable to unregistered labour	2.1	1.9	1.7	1.7
Illegal activities	0.4	0.4	0.4	0.4
- pimping	0.04	0.04	0.04	0.04
- drugs	0.37	0.29	0.31	0.34
- cigarette smuggling	0.01	0.02	0.02	0.01
Industry	1.4	1.4	0.7	1

[153] Aneks 3. Szara gospodarka i działalność nielegalna…, p. 100, Cf. J. Fundowicz, K. Łapiński, B. Wyżnikiewicz, D. Wyżnikiewicz, *Szara Strefa 2022,* p. 14,
[154] Aneks 3. Szara gospodarka i działalność nielegalna…, p. 100,

Construction	2.3	1.7	1.7	1.8
Trade in and repair of motor vehicles, accommodation, catering	5.2	4.8	4.7	4.4
Transport and storage	1.0	1.1	1.2	0.9
Real estate market services	1.5	1.7	2	1.5
Other sections	1.5	1.4	1.4	1.1

348. The shadow economy estimates provided by Statistics Poland concern the period until 2019. Different forecasts of the shadow economy were indicated by the Institute of Economic Forecasting and Analysis (IPAG) in the cited Shadow Economy 2022 report.

349. The IPAG presented in the report the following estimates made by it in accordance with the Statistics Poland methodology:

Table 19. IPAG estimates regarding the shadow economy (Statistics Poland data) for 2020-2022

Estimates of the size of the shadow economy (according to Statistics Poland) in GDP in 2020-2022	**2020**	**2021**	**2022**
GDP (PLN billion; source: until 2021 – Statistics Poland, 2022 – IPAG forecast)	2,327	2,603	2,904
Non-observed economy (PLN billion; IPAG estimates)	282	320	372
Share of the shadow economy (IPAG estimates)	12.10%	12.30%	12.80%

350. In its estimates, the IPAG included data that Statistics Poland does not (according to the IPAG) takes into account sufficiently, such as:

- unregistered transactions on the trading market, including: illegal fuel trade, some marketplace trade, some cross-border trade, some e-commerce,
- income from illegal gambling,
- educational services, such as tutoring or writing commissioned diploma theses,
- illegal mining of minerals such as gravel and sand, and exploitation of amber deposits,
- trade in forest groundcover, illegal breeding of purebred animals, illegal logging, etc. activities related to agriculture, horticulture or forestry,
- trafficking in steroids, counterfeiting drugs, manufacturing illegal weapons, etc.,
- effects of unregistered economic activity of citizens of other countries in Poland, mainly Ukraine.

351. According to the IPAG, the total value of the shadow economy in Poland will amount to PLN 590 billion in 2022. In 2018–2022, the added value of the shadow economy according to the IPAG approach will increase by a total of PLN 181 billion. The Institute forecasts that in 2022 alone, the total increase in value added in the shadow economy will amount to PLN 79 billion.

352. Ultimately, the IPAG provided the following estimates of the unregistered economy:

Table 20. Estimates of the unregistered economy according to the IPAG for 2020-2022

Estimate	2020	2021	2022
Value of the shadow economy (IPAG approach; PLN billion)	449.00	511.00	590.00
GDP adjusted for the shadow economy according to the IPAG	2,494.00	2,794.00	3,122.00
Share of the shadow economy in adjusted GDP	18.00%	18.30%	18.90%

353. It follows from the above that in Poland, there may be significant resources of unregistered money that entities generating it may try to introduce to circulation.

354. According to this approach the market environment has failed to satisfy the needs a given entity is trying to satisfy through the shadow economy. It was pointed out that participation in this segment of the economy is voluntary, i.e. the unregistered transaction between two participants is consensual. This solution benefits both parties[155]. The study indicates that in Poland, the shadow economy was growing just like the economy. The difference is that the Polish economy developed faster than the shadow one. This gave the false impression that the unregistered economy was shrinking. After 2008, a decrease in its monetary value can be observed, to remain at a similar level in the following years[156]. The document notes that research on the shadow economy is difficult due to the unobservable nature of this phenomenon[157].

The document lists a number of industries at risk of shadow economy development, including:

- waste industry. It was noted that a considerable progress had been made in this field, but a number of problems were also noticed, such as lack of a single, centrally managed database where information on collected and recycled waste would be collected. An increased risk of circumvention of increasingly restrictive waste disposal regulations was pointed out[158]. The shadow economy in this segment of the economy is estimated at 30-40%, i.e. approx. PLN 6 billion annually[159],
- gambling industry. The study indicates that in the Polish gambling industry, the share of entities conducting strictly criminal activities is not the same as in Western and Asian countries. Still, such entities constitute a fundamental threat in Poland. These are not mafia-like entities, but organised groups that benefit in various ways from organising illegal gambling games. This applies in particular to entities registered in countries with favourable conditions for offering gambling services, operating on the Internet, that created, through active marketing campaigns, the impression of legal operation. In recent years, there has been a noticeable increase in budget revenue from taxes and fees paid by entities from the gambling industry. It was pointed out that action should be taken to increase supervision over entities offering gambling games and over granting licences and permits. Introducing a central list of trusted entities and educating the public on legal gambling is also necessary, so is increasing cooperation and coordination of activities in eliminating illegal operators. It was

[155] Przeciwdziałanie szarej strefie w latach 2014 – 2022, UN Global Compact Network Poland, p. 38
[156] Przeciwdziałanie…, p. 40
[157] Przeciwdziałanie…, p. 129
[158] Przeciwdziałanie…, **p**p. 45-46
[159] Przeciwdziałanie…, p. 47

ultimately concluded that compared to other markets, relatively few undesirable phenomena can be observed in the gambling industry[160],

- liquid fuels and used oils industry. The document indicates that in 2012 alone, the share of VAT fraud in the industry concerned was 12.6%. The tax loss on this account was estimated at PLN 6 billion in 2013 and as much as PLN 10 billion in 2015. According to the Polish Chamber of Liquid Fuels, in 2014, losses attributable to the shadow economy were estimated at PLN 7.85 billion. It was indicated that the fuel industry was a sector particularly exposed to criminal activities. The growth of the shadow economy in this market segment was stopped after 2016, when a "fuel package" and an "energy package" were introduced and additional steps were taken, i.e. inspections were intensified, the method of bonusing the officers involved was modified, the mechanism for paying tax on fuel imported to Poland was changed, etc. This resulted in an abrupt increase in demand for legal fuel. In 2016-2018, diesel consumption increased by 15-17% annually, which was related to curbing the shadow economy. As regards waste oils, there are problems related to marketing liquid fuels produced from used oils, or their use contrary to their intended purpose, e.g. as wood impregnations. State budget losses on this account are estimated at approx. PLN 150 million annually, and this amount is considered underestimated. Problems identified in this market segment included the lack of an effective primary market control mechanism, the lack of a mechanism ensuring the actual collection of goods of this type by the end customer (which may result in illegal consumption, e.g. for heating purposes), and the lack of a mechanism forcing the actual use of the product in accordance with its intended purpose[161],
- spirits industry. The study indicates that this market segment is still susceptible to shadow economy activities, which includes both the illegal production and distribution of alcohol products. Particular losses for the state budget are generated by the denatured alcohol market, where ethyl alcohol produced from denatured alcohol is placed on the market. Other major problems include the illegal production of alcohol, i.e. moonshining, and alcohol smuggling. On the plus side, there has been a change in social habits resulting in a reduced demand for alcohol and a change in drinking culture, i.e. switching to products with lower alcohol content, most of which are produced locally, by legally operating entities[162],
- tobacco industry. The study indicates that the increased pressure of public administration on shaping healthy attitudes in society increases the profitability of illegal trade in tobacco products. A greater share of taxes in the price of the final product increases the margin and benefits of entities operating illegally. The major threats recorded on the market include smuggling and illegal production of tobacco products. Moreover, there are products on the market that have been taken away from legal factories. Regulations have covered also innovative products, i.e. electronic cigarettes and tobacco heaters, which increases the risk in this segment. It was pointed out that the effectiveness of combating smuggling and detecting illegal production locations increases every year. It was ultimately indicated that the share

[160] Przeciwdziałanie…, pp. 62-67
[161] Przeciwdziałanie…, pp. 72-79
[162] Przeciwdziałanie…, pp. 82-85

of the shadow economy in this industry is estimated at 4.9% and is considered the lowest in the European Union,

- electrical and electronic equipment industry. The document indicated that trading in electronic equipment was one of the tools most often used to organise carousel crime. The goods used in such offences were placed on the market in Poland, where, taking advantage of the lower price (the goods were free of taxes and customs duties), they displaced the goods of legal sellers. Another threat was posed by increasing the volume of purchases via Asian purchasing platforms, where, taking advantage of the policy to support postal operators by some Asian countries, it was possible to purchase large quantities of electronic equipment at a low price. Abuse of regulations regarding limits on the value of shipments and the lack of sufficient control by customs authorities resulted in the introduction of large quantities of cheap consumer electronics into Poland. Changes in the method of controlling taxation of transactions in the electronics industry, introducing the so-called e-commerce package, construction of a foreign shipment control centre and other measures have curbed shadow economy activities in this area. At the same time, the unsolved problem of electronic waste was pointed out[163],
- catering industry. The study indicates that the catering industry experienced major problems due to the COVID-19 pandemic, followed by the increased inflation, which resulted in reduced consumption. These factors have resulted in the growth of the shadow economy and the inhibition of the downward trend observed in it until 2020, whereby the catering activity is clearly associated with the shadow economy manifested in different ways, including lack of fiscalisation of sales, illegal employment, concealing income from tips, etc. Another problem is social acceptance of such practices and the lack of customer awareness. As for positive trends, an increase in the number of non-cash transactions is recorded[164],
- construction industry. The share of the shadow economy in this industry is obvious, and due to the size of the market, shadow market activities generate significant amounts of unrecorded revenue. Illegal employment, circumventing labour law, remains the main risk in this area. As a result, a significant number of entities operate unofficially, and thus do not record their income. Lowering quality, forging certificates or even stealing construction materials are other problems. Construction materials, e.g. ribbed bars, have been involved in carousel crimes. The situation is aggravated by social acceptance of such practices, as customers often seek to reduce the costs of expensive projects, and the common practice of using the lowest price criterion in public tenders[165],
- trade in counterfeit goods. Such products most often come from Asian countries, arriving usually via post and courier shipments. The document indicates that despite regulatory and control steps, counterfeiting goods remains a major problem (referred to in the document concerned as *"mass and deeply rooted"*). This illegal practice most often concerns clothing, watches, jewellery and cosmetics. Besides luxury goods and consumer electronics, counterfeit food is also on the rise. As far as

[163] Przeciwdziałanie…, pp. 90-94
[164] Przeciwdziałanie…, pp. 94-99
[165] Przeciwdziałanie…, pp. 100-103,

counterfeiting intellectual property rights is concerned, it is mostly manifested in large-scale counterfeiting of trademarks, e.g. by sewing counterfeit labels on unbranded clothes. The document indicates at this point social consent of consumers who want to buy branded products they cannot afford. Insufficient judicial protection of entities administering given intellectual property was also highlighted[166],

- pharmaceutical industry. The document indicates that state authorities are taking action to combat reverse sales of medicines by pharmacies to wholesalers and the export of medicines abroad. A number of legislative actions have been taken against these practices, including clarification of the obligations of entities involved in the trade in medicinal products, clarification of the provisions on the online sale of medicines, increasing the control powers of pharmaceutical inspectors, and penalisation of participation in the trade in medicines from such sources at every stage. Another dangerous phenomenon consists in drug smuggling and counterfeiting, facilitated by the development of online sales channels[167],
- coal trade. In Poland, there is a significant demand for this type of fuel. Domestic mining output is consumed mainly by power plants and industrial plants adapted to use this particular type of coal. The demand of households using fuel for heating purposes is met with imported coal. The introduction of an embargo on imports of coal from Russia, subsequent shortages of coal on the market, and state intervention in market prices have been resulted in speculation and illegal trade in this commodity. Irregularities include the sale of coal that does not meet relevant standards, secondary sale of coal purchased at guaranteed prices, and an increased incidence of fraud in distance purchases[168],
- road transport of passengers. The document indicates that there is a threat related to the development of shadow economy activities in the transport of passengers from beyond the eastern border. The destabilisation related to the war in Ukraine resulted in the risk of an influx of people posing a threat to state security, e.g. by carrying out activities related to the expansion of the shadow economy or seeking to destabilise the social and economic situation in the European Union. However, due to the small scale of this phenomenon, it has not received adequate attention so far. Due to the small scale of this phenomenon, its observation generates high costs. This situation may be conducive to the development of a black economy in the future[169],
- shadow banking. The document indicates that subsequent market regulations did not affect entities conducting illegal usury activities. Such activities violated customers' rights in various ways, among other by violating consumer rights, legal protection, and in extreme cases, intimidation and extortion. Such entities also bypass the tax system. The study notes that the shadow economy in this sector is likely to grown due to market trends such as slowdown in the growth rate of wages, limited lending, reduced GDP growth, etc.[170]

[166] Przeciwdziałanie…, pp. 104-110,
[167] Przeciwdziałanie…, pp. 110-111,
[168] Przeciwdziałanie…, pp. 112-115,
[169] Przeciwdziałanie…, pp. 118-121,
[170] Przeciwdziałanie…, pp. 122-125,

355. Restrictions on cash payments were indicated as one of the tools to combat the shadow economy, while noting social resistance to this solution. The most important tools introduced in recent years to limit the non-observed economy were also indicated, i.e. the Standard Audit File, the establishment of the National Revenue Administration, and the introduction of the SENT system and the so-called transport package.

356. According to various estimates and analyses, the value of the shadow economy in 2019 ranged from 13.55% to 17.2%. However, with the onset of the COVID-19 pandemic and Russia's aggression against Ukraine, a number of unfavourable phenomena conducive to the growth of the shadow economy have been observed. Increased inflation has caused consumers to look for cheaper sources of goods and services. The economic slowdown has also increased the profitability of evading tax law. According to the estimates of UN Global Compact experts, the level of the shadow economy in Poland expressed as a percentage of GDP may exceed 20.65% of Polish GDP in 2022. The document notes that the programme to counteract shadow economy implemented in 2014-2020 helped limit this increase[171].

357. It is difficult to determine for statistical purposes what financial flows are considered illicit. The UNODC Conceptual Framework For The Statistical Measurement Of Illicit Financial Flows defines illicit financial flows as financial flows that are illicit in origin, transfer or use, that reflect an exchange of value and that cross country borders. The following key features can be attributed to such transactions:

- a flow of value is illicitly generated, illicitly transferred (e.g. violating currency controls) or illicitly used. According to this approach, any transfer that can be attributed to at least one of these features can be considered illicit,
- an exchange of value comprises more than purely financial transfers, but also, for example, cross-border bartering or the exchange of illegal services for other illegal services,
- illicit financial flows measure a flow of value over a given time,
- flows are cross-border ones. This includes assets that cross borders and assets where the ownership changes from a resident of a country to a non-resident, even if the assets remain in the same jurisdiction.

358. Financial flows originating from illegal economic activities can be carried out in such a way as to make subsequent transactions appear legal. It is challenging to determine the illicit origin of certain financial flows as the distance from the illicit origin increases. Funds from legal sources can also be illicitly used. Specific financial flows may be deemed illicit based on actors involved, channels, sources, etc.[172]

In the information on the findings of audit No. P/18/037/KPB, the Supreme Audit Office indicated that there is no coherent system for disclosing and seizing property and assets derived from crime. During the audit, it was found that all entities involved in the seizures had appropriate tools to perform these tasks. Nevertheless, coordination and assessment of the efficiency of the process are missing, so is ongoing exchange of information between these

[171] Przeciwdziałanie…, p. 129,
[172] Conceptual Framework For The Statistical Measurement Of Illicit Financial Flows, UNODC/UNCTAD, October 2020, pp. 12-13,

entities, which makes the system inefficient. There is also no document specifying long-term activities in the field of property and asset[173] recovery[174]. After analysing the audit concerned in terms of the activities of the Central Investigation Bureau of the Police, these findings are no longer valid. Property and asset disclosure and recovery are regulated by Decision No. 136 of the CBŚP Commander of 26 June 2019 on the procedure for property and asset disclosure and seizure to be followed at the Central Investigation Bureau of the Police. As part of the aforementioned regulation:

- a system of coordinators for property and asset disclosure and recovery has been developed,
- the method and scope of carrying out and documenting tasks have been standardised,
- a system of supervision and coordination of activities in this area has been introduced.

The trend in the value of property/assets seized by the Police, including the CBŚP, in 2020-2022 is described in the table below:

Entity	**Value of property/assets seized in January – December 2020**	**Value of property/assets seized in January – December 2021**	**Value of property/assets seized in January – December 2022**
TOTAL Voivodeship Police Headquarters/Metropolitan Police Headquarters	1,191,270,384	1,123,801,445	1,400,609,303
Central Investigation Bureau of the Police (CBŚP)	**692,248,334**	**704,105,949**	**760,242,562**

In the first half of 2023, property and assets worth PLN 404,523,395 were seized in cases conducted by the CBŚP.

359. The Polish system for counteracting money laundering observes a significant part of transactions in which these funds are used. In accordance with the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, in previous years, the GIFI received suspicious activity reports (SAR) provided in accordance with Article 86 of this Act. In 2022, 4,505 SARs were submitted. In 2020 and 2021, 3,805 and 3,852 such reports were submitted, respectively. The submitted reports also included ones containing information on single transactions selected by obligated institutions, that were not necessarily related to money laundering or financing of terrorism, referred to as suspicious transaction reports (STR).

[173] The Supreme Audit Office indicated that the average criminal proceeds in Poland in 2014–2018 are estimated at PLN 340.4 billion (approx. 3.6% of GDP), while the value of actually seized property and assets in this period was only PLN 2.7 PLN billion (approx. 0.8% of the estimated criminal proceeds).
[174] Information about the audit findings. Recovery of property and assets derived from crime, Supreme Audit Office No. KPB.430.009.2019, No. 158/2019/P/18/037/KPB, p. 14.

360. Pursuant to *Directive 2014/42/EU of 3 April 2014* Member States are required to introduce confiscation and extended confiscation, enabling the recovery of instrumentalities of crime and proceeds of crime. The data provided by the National Prosecutor's Office shows that in cases conducted in 2020-2022, property and assets were seized for the total amount of:

- in 2022 – PLN 2,305,096,051.53,
- in 2021 – PLN 1,609,253,130.96,
- in 2020 – PLN 1,989,388,485.79.

361. The inability to precisely determine the value of cash flows related to the shadow economy makes it also impossible to clearly determine the actual value of laundered revenue. Due to the informal nature of the transactions made there will always be doubts as to the actual value of this type of revenue. Any attempt to determine these values can only be estimates. At the same time, the authors of all studies agree that the shadow economy will grow in the near future.

362. According to Statistics Poland data, in 2016-2019, the proportion of strictly illegal activities in generating GDP was constant and amounted to 0.4% of GDP, but this estimate was based on information regarding only three types of illegal activities.

363. A more complete estimate of the amount of criminal proceeds that may subsequently be laundered can be calculated using the information contained in Revision of the EU rules on asset recovery and confiscation[175]. According to this document 2.2% of the total estimated proceeds of crime is frozen, and 1.1% of them are actually confiscated. Assuming that the above figures hold true also for Poland and using data provided by the National Prosecutor's Office, the value of the illegal economy can be estimated at:

- in 2022 – approx. PLN 104,775,093,251.36 (the amount calculated with the assumption that the value of proceeds frozen in 2022, i.e. PLN 2,305,096,051.53, constitutes 2.2% of total proceeds, at the rate indicated by EUROPOL),
- in 2021 – approx. PLN 73,147,869,589.09 (the amount calculated with the assumption that the value of proceeds frozen in 2021, i.e. PLN 1,609,253,130.96, constitutes 2.2% of total proceeds, at the rate indicated by EUROPOL),
- in 2020 – approx. PLN 90,426,749,354.09 (the amount calculated with the assumption that the value of proceeds frozen in 2020, i.e. PLN 1,989,388,485.79, constitutes 2.2% of total proceeds, at the rate indicated by EUROPOL).

364. Based on the above data, the average value of assets originating from the criminal economy in 2020-2022 can be estimated at approx. PLN 89,450,570,732. It can be therefore concluded that the estimated average amount of assets derived from criminal activity in the aforementioned period was 3.34% of GDP[176].

[175] https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739373/EPRS_BRI(2023)739373_EN.pdf, p. 2,

[176] The above estimates are close to global ones. The International Monetary Fund, citing the UN, presented these estimates at the level of approx. 2-5% of global GDP. In turn, the United Nations Office on Drugs and Crime indicated in one of its analyses that the total value of proceeds from crime, excluding those related to tax evasion, was approx. 3.6% of global GDP in 2009 (including approx. 2.7% of proceeds "available for money-laundering"). Moreover, in 2020, the High-Level Panel on International Financial Accountability, Transparency and Integrity (FACTI Panel) also presented estimates indicating that approx. 2.7% of global GDP is laundered annually.

5.3 MOST COMMONLY USED MONEY LAUNDERING METHODS

365. The goal of criminals is to introduce "dirty money" into official circulation by means of actions that do not stand out from the behaviour of legally operating natural persons or businesses. Various methods of money laundering comprise specific activities performed by the aforementioned entities that legalise money derived from crime in this way.

366. Although particular methods can be used on their own, they are often combined to create a multi-dimensional and multi-method way of legalising "dirty money" or allocating funds for terrorist activities. After all, it is all about hiding the source of the money and its intended use as best as possible.

367. Some of the most well-known methods of money laundering involve the use of bank accounts (as well as other payment accounts). These are:

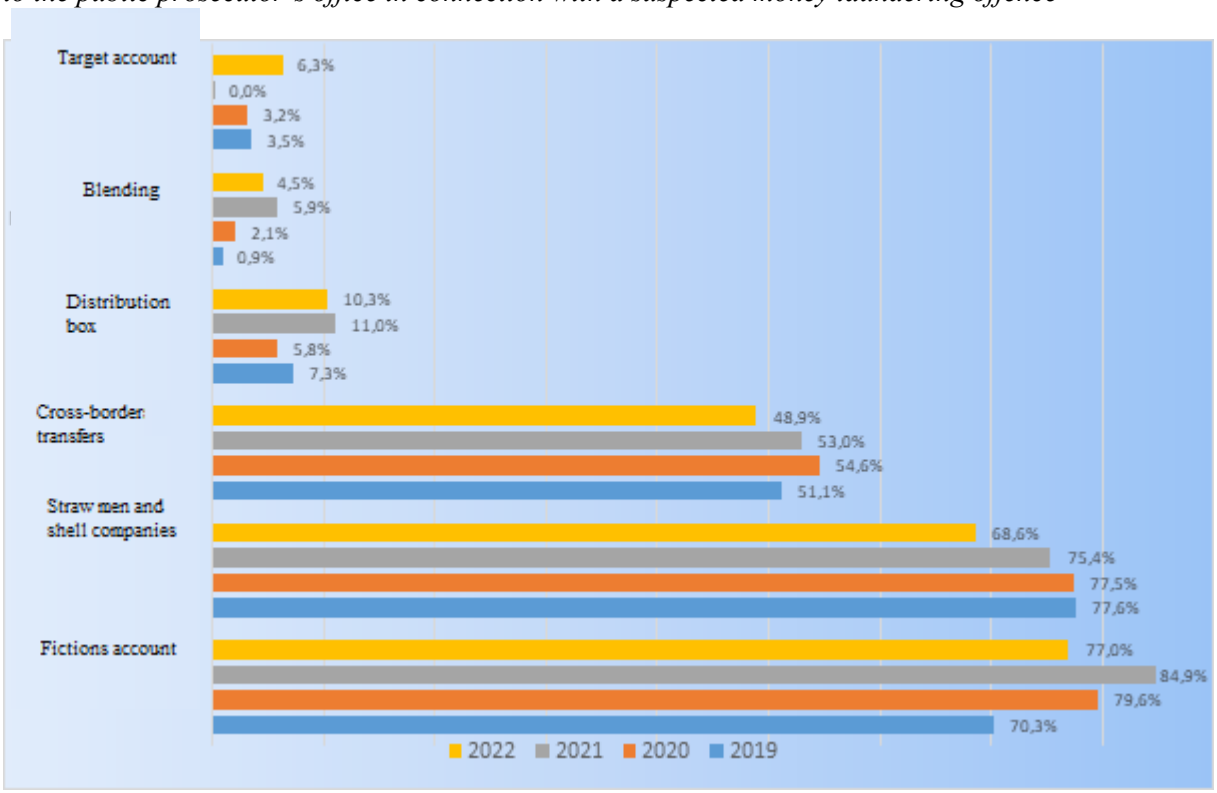
- *"fictitious account"* (a method consisting in opening an account to complete one or several transactions at short intervals, for very high amounts, using a maximum number of fictitious elements, e.g. forged documents presented when opening the account, providing a false purpose for opening the account or false purposes of the ordered transactions),
- *"cross-border transfers"* (a method consisting in using cash transfers to transfer assets between different jurisdictions),
- *"distribution box"* (a method consisting in 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 consisting in transferring large amounts to a single account – often operating for a relatively short time, from which they are immediately withdrawn in cash),
- *"pass-through account"* (a method consisting in crediting an account using transfers coming mainly from one source in order to immediately transfer the thus obtained funds to another account).

368. Based on the content of notifications on a suspected money laundering offence submitted to the prosecutor's office by the GIFI in 2019-2022[177], it can be concluded that the methods most frequently identified in analytical proceedings conducted by the GIFI included – apart from the "straw men and shell companies" method – methods such as "fictitious account", "cross-border transfers", "distribution box", "target account" [178] and "pass-through account".

[177] The reference is made to main notifications. Besides them, the GIFI forwards to the prosecutor's office also supplementary notifications, sent following the 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 has followed.

[178] It follows from the GIFI's experience that the "target account" method often involves the use of tax-exempt entities.

Chart 5. Percentage of the identified use of particular money laundering methods in all identified money laundering methods based on the content of the main notifications submitted by the GIFI in 2019-2022 to the public prosecutor's office in connection with a suspected money laundering offence



369. The *"fictitious account"* method involves the use of an account that has been opened and actually exists, but the purpose of its opening is fictitious. A fictitious account is an account that has been opened to make one or several transactions at relatively short intervals, often for relatively high amounts. An account that has previously remained dormant may also be used to make a transaction. Money laundering on a fictitious account is carried out both through very simple operations (e.g. cash deposit and withdrawal) and more complex ones (e.g. several transfers between fictitious accounts that end with a cash withdrawal). In the case of such a chain, it is worth paying attention to decreasing transfer amounts, which is due to cash withdrawals made by "holders" of fictitious accounts, being a commission for the money laundering service. The commission amount is a few percent of the amount of money laundered. The "fictitious account" method is often used in cases involving the laundering of money from VAT fraud. In such cases, bank accounts are opened to carry out – in a relatively short period – financial transactions aimed at confirming the flow of cash for the purchase of goods, while making it difficult to trace money from unpaid VAT. The above method is also used to launder money from other types of offences.

Example 1

A certain limited liability company /1/ was a client of a cooperative bank. For the first two months, the balance on the account kept in its name did not exceed PLN 400. After this period, the company's account was credited within five days with more than PLN 1 million via five

transfers. All transfers came from a single source (another limited liability company /2/) and amounted to equal amounts of PLN 250,000 each. The transaction was made as "payment for an invoice". The transferred amounts were each time withdrawn in cash by the owner of limited liability company /1/. The withdrawals were made on the same day as the account was credited through transfers. After the last transaction was made, the account owner no longer showed up at the bank. One of the bank employees went to the address indicated in the account agreement and found that there was no company operating at this address, and the premises allegedly occupied by limited liability company /1/ were inhabited by an elderly person.

Example 2

The case concerns irregularities in the application of tax regulations by a group of companies belonging to several persons connected with each other through business relationships, consisting in placing industrial goods imported from Asian countries on the Polish market by several leading companies, without properly settling VAT and burdening the other group participants with liabilities arising from this tax, as a result of which civil law receivables towards the State Treasury were significantly depleted. The proceedings in the case are being conducted by one of the Regional Prosecutors' Offices. The illegal practice involved several limited liability companies and joint-stock companies operating in various industries, among which the dominant role was played by several main companies registered in Silesia or Warsaw, belonging to a narrow group of several people connected to each other through business relationships, operating as online currency exchange platforms, companies dealing with wholesale imports of goods from Asia, conducting brokerage activities, activities related to investment consulting and IT consulting. The remaining companies participating in the illegal practice usually belonged to other natural persons, including employees of the main companies, as well as persons playing the key role in the illegal activities. Those in charge of the illicit dealings were also the owners of a Cypriot company through which the funds were transferred to the accounts of the Polish companies. The accounts were also credited with funds introduced to the circulation as an increase in the capital of the companies through trading in shares. Then, these funds were repeatedly transferred between the accounts of the companies participating in the illegal dealings. Transfers, apart from titles indicating the settlement of invoices, were often vaguely described, for example as "transfer", "own payment", or concerned loans granted by one of the owners of the leading companies; transfers related to loans granted to or on behalf of this person, in various amounts, were made to many accounts, to be finally transferred to the personal account of the person they concerned or to the account of the Cypriot company. In this case, the GIFI sent 4 notifications to the Regional Prosecutor's Office and blocked 21 accounts.

Example 3

In September 2019, the GIFI was analysing a case based on information received from the prosecutor's office about ongoing proceedings supervised by it, initiated based on a notification from the tax authority. According to the information provided by the prosecutor's office, it was supervising an investigation into an organised criminal group operating in Poland since 1 January 2017 or earlier, that committed offences against economic transactions and fiscal offences, involving, among others, concluding fictitious contracts documenting the provision of services that did not actually take place and issuing false invoices for at least PLN 24.6 million. The aforementioned group also derived financial benefits from its VAT returns that did not

correspond to the actual turnover and from failing to submit VAT returns, which led the State Treasury to unfavourable disposal of property through refunding tax to certain entities for an alleged overpayment of goods and services tax. According to the information provided by the prosecutor's office, the group included Ukrainian citizens acting on behalf of several limited liability companies. Moreover, according to the information from the prosecutor's office, one of these individuals made punishable threats towards another person in September 2019. The Police confirmed at the scene of the incident the presence of two firearms and ammunition held without a relevant permit. The person making the threats fled before the Police arrived and tried to escape from Poland. This person was in possession of a significant amount of cash, valuables in the form of gold and icons, as well as computer equipment and a mobile phone. In October 2019, the GIFI sent a notification to the prosecutor's office on suspicion of money laundering by three Ukrainian citizens acting on behalf of one of the companies. The analysis of the bank account showed that the company received cash from various entities in the amount of nearly PLN 14 million over a two-year period. The accumulated funds in the amount of nearly PLN 9 million were paid out in cash. According to the notification, the Ukrainian citizens accepted funds paid into the bank accounts and then withdrew them in cash in order to conceal their criminal origin. The General Inspector of Financial Information blocked approx. PLN 0.2 million. Following the aforementioned notification, the GIFI received another letter from the prosecutor's office from which it followed that, among others, after the GIFI blocked the company's account, identified individuals took action consisting in substituting contracts and invoices for work performed by the employees of that company and indicating a new bank account for payments, which, according to the prosecutor's office, was aimed at redirecting payments and siphoning money from the company, bypassing the blocked account. It was suspected that these funds could be transferred to Ukraine. In the course of the analysis of the materials held by the GIFI, in November 2019, the GIFI sent to the prosecutor's office another notification in this case regarding the president of the management board of the company whose account had been previously blocked. The GIFI found that the account indicated in the substituted contracts and invoices was opened by the president of the management board three days after the GIFI had blocked the company's account. It should be noted that the business partner, when ordering transfers to the personal account of the president of the management board, indicated the company as the payee. The balance on the account on the day it was blocked was PLN 0.3 million. In 2020, the GIFI received information from the prosecutor's office that the funds blocked in the accounts were recognised as material evidence for the case conducted by the prosecutor's office. Moreover, the prosecutor's office communicated that money laundering charges had been brought against two Georgian citizens who, in agreement with other individuals participating in the organised criminal group, withdrew funds from ATMs, which made it much more difficult to determine their criminal origin and location. In October 2020, the Police informed the GIFI that in connection with the proceedings supervised by the Prosecutor's Office, under which the GIFI sent the notifications, gold products and works of art (icons) for a total amount of PLN 1 million were seized during the activities performed in October 2020. It was also communicated that the prosecutor's office blocked the suspects' accounts in October 2020.

370. The "straw man" and "shell company" method. "Straw men" are natural persons recruited by criminals to open bank accounts and establish powers of attorney for company accounts. Such individuals, who are often in a difficult financial situation, lend their personal

data for a certain fee to carry out these activities and legitimise activities related to these companies and accounts. They usually have no impact on the actions and transactions taken. Their possible contacts with public authorities as well as credit and financial institutions connected with the operation of "shell companies" and bank accounts are strictly controlled by criminals. This method is one of the most frequently used by criminals and organised criminal groups.

371. "Shall companies" are usually companies or natural persons registered as entities conducting business activities that are controlled by criminals. The purpose of their activity is to simulate legal business conduct as a cover for carrying out transactions aimed at introducing funds from illegal activities into economic transactions. Perpetrators often create complex and long chains of organisational and ownership connections between this type of business entities and associations, charities, trusts (with the involvement of entities registered in various jurisdictions, including tax havens) in order to make it difficult to identify the beneficial owners of entities used for money laundering. "Shell companies" are often established and operated using the services of "virtual offices". This involves the use of specialised individuals and companies to carry out the procedure related to establishing a company, as well as providing office services without the need for the company's physical presence at the declared registered office.

372. There are three types of "shell companies". The first one includes *primary shell companies*, i.e. business entities with a simple organisational structure, or more precisely, natural persons running a business, recruited to register a business and open a bank account used exclusively for money laundering, The second group includes *acquired shell companies* that are usually commercial law companies established earlier by individuals who actually intended to run a business. As a result of discontinuation of business activity or the threat of bankruptcy, shareholders are interested in selling shares to third parties and thus obtaining some profit from an already unprofitable enterprise. In the case in question, shares in such companies are bought by straw men designated by organised criminal groups or members of these groups themselves. Taking control of such a company gives the opportunity to create the appearance of greater credibility as a new bank client – the company has been operating for some time, the company's name is known, there is no need to register a new business, etc. The practice of company acquisition, known for generating fictitious costs of running a business to take advantage of tax deductions, is now equally successfully used by money launderers. As for the last group, these are *intermediate shell companies* that include companies that besides their legally conducted business activities, make transactions aimed solely at laundering money, e.g. the management board of a company dealing with legal trade in fuels decides to use the company's name to legalise "dirty money" through its accounts. This category of shell companies uses a money laundering method called "blending", whereby the "dirty money" is not the company's income, but it is transferred to the accounts of other entities forming an organised criminal group.

Example 1

A new customer came to a bank branch to open a foreign currency account. A day later, another person came to another bank branch and opened an identical bank account. Immediately after their opening, the accounts of both individuals were credited with cash deposits in identical amounts of USD 10,000. In both cases, on the day of transfer, it was ordered to transfer the

funds concerned to the same non-resident. These facts would not have been linked if it had not been for the same data of the non-resident payee, the attempt to repeat the payment and transfer pattern, and the refusal of one of the individuals to have his identify verified by the bank. Verification of the declared income of both natural persons confirmed the suspicions that these persons acted as "straw men". The funds they deposited into their accounts came from third parties.

Example 2

Money laundering through a crowdfunding platform. One of the crowdfunding platforms where unrelated people can raise money for a specific purpose defined by the founder of the fundraiser, noticed that some people operating on the platform may launder "dirty money" originating from unauthorised access to stolen debit and credit cards. The crime pattern was as follows: a bank account was opened for straw men and a fundraiser was opened. In the analysed case, a Georgian citizen was a straw men (A), and the fundraiser was to help animals. The fundraiser account was credited with several transfers from the aforementioned cards. The raised funds were then transferred to the account of another natural person – also a straw man (B). The platform was approached by an aggrieved person from whose card unauthorised transfers were made. All payments probably came from stolen cards. Following a thorough analysis of the content of the fundraiser and its description, it was concluded that it was unlikely that people from other countries would make payments to a fundraiser whose description/purpose, written in Polish, contained a lot of grammatical/stylistic errors. Thanks to the cooperation between the platform and the payment system provider, the GIFI managed to block some of the funds originating from crime. This was the first case disclosed in Poland where a crowdfunding[179] system was used as a tool to launder money.

Example 3

The case concerned an attempt to obtain money from Poczta Polska S.A. by false pretences through the fictitious operation of a postal operator agency ("shell company"). Several transfers for the total amount of PLN 4 million were made to the account of a natural person ("straw man") opened with one of the banks. In the course of the analysis and collection of information from the ordering party's bank, the following circumstances were established: in a newly opened postal operator agency ("shell company", a contract concluded a few days earlier), fraud involving booking fictitious cash payments for a total amount exceeding PLN 14 million for the sale of land (as stated in the notarial deed) was most likely committed. The funds from fictitious payments at the postal operator agency ("shell company") were then transferred to the account of a natural person ("straw man") and then partially transferred to other accounts of that person opened with other banks. It was established that the aforementioned postal operator agency ceased to operate immediately after the described transactions were carried out (the case of the postal operator agency was reported to the Police by Poczta Polska S.A.). The GIFI requested that the accounts with the funds in question be blocked and sent a notification to the competent prosecutor's office.

373. As part of the "cross-border transfers" method (transfers of funds via a bank account), both cash transactions linked and not linked to a payment account (e.g. a cash deposit combined

[179] A crowdfunding platform is a digital solution made available on the Internet to an open audience by a crowdfunding service provider, used to carry out fundraisers.

with an order for a cash withdrawal to another entity in another country) may be used. Sometimes funds transferred abroad using this method were transferred back to Poland after passing several stages of money laundering. This method consists of two stages: the first stage consists in crediting the account with cash (when making payments, the following techniques of introducing "dirty money" into financial transactions are often used: smurfing, structuring and blending), while the other stage involves making the deposited funds available to payees abroad (at this stage, the money can either be transferred to the accounts of designated payees or withdrawn abroad using payment cards transported across the border or delivered there in another way). While transfers to accounts abroad allow for large amounts of money to be delivered to the payee relatively quickly, withdrawals using payment cards are subject to daily limits set by the bank.

Example 1

Amounts ranging from EUR 10,000.00 to EUR 30,000.00 were paid in cash to the account of a company registered in one of the tax havens. The transaction were ordered by two natural persons (non-residents). One of them was also authorised to use the company's account. Information was obtained that both natural persons crossed the eastern border of Poland, declaring the import of large amounts of foreign exchange. The money paid into the account was then transferred to the accounts of two other companies in one of the European countries. According to unconfirmed data, the transferred funds could have been derived from trading in stolen cars.

Example 2

The case in question conducted by the GIFI concerned money laundering by a payment institution. The GIFI received a notification from an obligated institution as well as from a cooperating entity. The analysis showed that the payment institution had accounts with 9 banks in various currencies, that were used to make money transfers on behalf of the payment institution's customers to companies based in Asia. The customers included companies owned by Asian nationals. The payment institution received from the aforementioned companies significant amounts of cash in the form of cash deposits, but was unable to explain the source of these funds. Documents purporting to legitimise the source of these funds were also suspicious (they were not credible). During the analysis of the case in question, the GIFI identified several Asian citizens whom it had previously come across in the files regarding cases conducted by the Polish FIU (the GIFI sent a notification to the prosecutor's office regarding these persons and blocked their bank accounts). The GIFI found 90% of the financial transactions carried out by the payment institution concerned suspicious. The funds used therein came from tax offences. In connection with the findings made, the GIFI also used its control powers with respect to the activities of the aforementioned payment institution. The analytical and control activities resulted in two notifications sent to the prosecutor's office, in which 15 individuals suspected of committing tax offences were indicated. The prosecutor initiated an investigation and entrusted its conduct to the Central Anti-Corruption Bureau. The GIFI participated in a number of coordination meetings with the prosecutor and the Central Anti-Corruption Bureau. The GIFI was in possession of a great deal of information and documents that it shared with the prosecutor as requested. Further analysis of the case showed that the aforementioned payment institution conducted it activities in another country. The Polish FIU cooperated in this respect with the FIU in that country. Moreover, in cooperation

with the prosecutor's office and the Central Anti-Corruption Bureau, the GIFI requested that 16 bank accounts belonging to 10 suspects be blocked. It was found that 26 Asian companies participated in the scheme. The prosecutor's office charged 18 individuals with money laundering and participation in an organised criminal group. The organisers of the illegal activities were arrested. In total, over PLN 8.6 billion was transferred abroad, and the state budget lost PLN 2.3 billion. There are grounds to suspect that the money could also have come from other offences.

374. The "distribution box" method is characterised by crediting the account using various types of transactions (in particular cash deposits and transfers), originating from various sources (less often from a single source), in order to achieve a sufficiently high balance on the account and transfer the funds accumulated in it to another account or other accounts. This method uses both accounts kept for businesses and natural persons. When making payments to such accounts, other methods of money laundering, such as smurfing or structuring, are also used. This seemingly simple method has a number of undoubted advantages for launderers, such as the anonymity of the sources of money crediting the distribution box, especially when combined with smurfing and structuring, the option of ordering the bank to "automatically" make transfers to a specified account once a certain balance has been reached, and minor losses sustained by the launderer (throughout the operation) in case of suspension of the transaction or blocking of the account. Money laundering using the method concerned can be carried out both through very simple operations, consisting in crediting the account and making cash withdrawals by the person for whom the account (serving as a distribution box) is kept, as well as more complex ones, involving various sources and forms (cash, non-cash) of crediting the box, and electronic transfers are made to various entities, including ones based abroad. Moreover, it should be added that in the distribution box method, unlike e.g. the fictitious account method, transactions typical for "normal" business activities can be made using the account serving as a box, such as payments to the Social Insurance Institution (ZUS), salary payments, and transactions with entities participating in money laundering. The "distribution box" method enables the introduction of funds from illegal sources into financial transactions and their quick transfer to other places/locations. The use of this method is illustrated by the example below.

Example

The case was initiated with a notification submitted pursuant to Article 86 of the Act on counteracting money laundering and financing of terrorism, regarding the activities of a business managed by a foreigner. The foreigner's limited liability company conducting business activities purportedly in the accounting/bookkeeping and tax consultancy sector, claimed to provide services to a company from Eastern Europe to help it obtain a licence for an electronic money institution in Poland. The Polish company opened a new current account that soon began to be credited with funds from settlements made using POS terminals. The devices were used to receive payments from several payment cards issued by foreign banking institutions. Further analysis showed that these funds were then transferred, through a payment institution, to Western European companies whose names indicated that they operated in the pharmaceutical and electronics industries, with transfer titles relating to payment for cosmetics and consumer electronics. The pattern of transactions indicated the laundering of money originating from stolen cards or skimming. The GIFI decided to block the company's account.

Over the next few days, other institutions obligated under Article 74 and Article 86 of the Act on counteracting money laundering and financing of terrorism submitted notifications to the GIFI regarding the activities of two other companies managed by the same person. The institutions noticed to an abrupt increase in turnover after a period during which the POS was inactive. This activity increased after the first account was blocked. During the analytical procedure, the same transaction pattern was confirmed each time – crediting the account with funds from several foreign payment cards through a POS settlement, processing of the transactions to the bank accounts, and then transfer abroad using a payment institution. The GIFI requested that all accounts held for the aforementioned entities be blocked. The total amount of blocked funds was PLN 876,000.

375. The "target account" method. This method is characterised by transferring large amounts to a single account, from which they are immediately withdrawn in cash, also in the form of cheques. In this case cash withdrawal is the end of a predetermined "path" of money laundering. Transfers to the target account are obviously preceded by a number of steps (constituting an inherent element of the method concerned) aimed at making it difficult or impossible to determine the criminal origin of the funds. These steps may take the following forms: a chain of bank accounts through which funds are passed in order to be withdrawn in cash from the account being the last link in the chain, making transfers by various entities (also using "intermediary" accounts) to the same account from which any incoming funds are withdrawn in cash. It should be noted here that the aforementioned forms of actions in the target account method serve only as examples, that enable, however, the *modus operandi* of perpetrators to be captured. In practice, launderers create not one, but many chains of bank accounts between which transactions are also made, which means that the number of accounts from which funds are withdrawn in cash is obviously larger. A similar remark can be made with respect to the second example, as a group of money laundering entities can make transfers to many accounts from which funds are later withdrawn in cash. As for the second of the presented forms of using the "target account" method, i.e. using tax-exempt persons, it should be noted that very often the account from which the money is withdrawn is kept for an entity whose income is exempt from tax pursuant to Article 17 of the *Act of 15 February 1992 on corporate income tax* (Journal of Laws of 2022, item 2587). The use of a tax-exempt entity creates a very favourable situation for launderers, especially when siphoning money from businesses. Fictitious contracts are concluded between such entities and the tax-exempt entity, and then the tax-exempt entity issues invoices for the provision of, for example, a specific service. The account of this entity is credited with funds constituting payment for the provision of the purported service. These funds, less a commission of several percent of the laundered amount, are withdrawn in cash and thus laundered return to the entity (entities) that initiated the money laundering path. At the same time, such entity declares high tax-deductible expenses (a significant part of which is attributable to the cost of the purported service/services), and thus avoids paying high taxes, and often even declares a loss. When it comes to the tax-exempt entity, the amounts obtained for the purportedly provided service/services are, of course, declared in its tax returns as tax-exempt, in accordance with Article 17 of the aforementioned Act. Transactions on bank accounts are accompanied by the legitimisation of their implementation through the mutual issuance of invoices by the entities involved in the illegal operation for amounts equal to the amounts of the transfers. In the case of a well-organised operation, transfer titles contain entries referring to specific numbers of previously issued

invoices. Speaking of invoice circulation, it is worth mentioning a certain form of money laundering where the laundered funds are physically transferred between the organisers of the illegal operation, and this transfer is accompanied by invoice circulation driven by a chain of entities issuing them. In this case, however, the issuance of invoices is not accompanied by the turnover of funds on these entities' accounts. In the case of the "target account" method, it can even be said that its effectiveness is largely dependent on the use of auxiliary methods. These methods include the use of "straw men", "shell companies", structuring, and entities exempt from income tax.

376. The "blending" method. This method involves blending income from legal business activity with assets from illegal or undisclosed sources. It is one of the simplest methods of money laundering and, apparently, the least expensive. This method is particularly easy to use when running a business whose income, e.g. daily or monthly, is difficult to predict. Blending can take place:

- as part of a legally conducted business activity, dependent on criminal groups (voluntarily or under violence),
- as part of business activity conducted by a criminal group.

Given the characteristics of this method, it is used most often where income results from cash receipts, e.g. in the catering industry.

377. *Bank loans and credits.* The basic variant of the money laundering method using bank loans and credits involves obtaining a credit (or a loan) that is then repaid using money from illegal sources. Repayments may be made by third parties on behalf of the borrower. Loans are easier to obtain because the customer does not have to meet as many conditions as in the case of a bank credit (e.g. in the case of businesses: business plans, notarial deeds, certificates, financial statements, etc.) and specify the appropriation of the money, but their costs are higher. Like any money laundering method, this one also has more complicated mutations:

- loans and credits with collateral on assets or property originating from criminal sources. Natural or legal persons obtain credits and loans by putting in deposits made of money from illegal sources or real estate, or movable property purchased for criminal proceeds as collateral. It should be noted that collateral may be put in by an entity other than the borrower, e.g. a foreign company based in one of the "tax havens". For example, criminal proceeds are transferred to a foreign company and then return to Poland as transfers to this company's account with a Polish bank or contributions to investments (e.g. for the purchase of real estate). These assets further serve as collateral for credits and loans obtained by the aforementioned Polish natural or legal persons. In this way, criminals end up with funds from a definitely legal source, i.e. a bank. Credits and loans may be repaid by taking over by the bank the collateral in the form of property and assets originating from an illegal source,
- refinancing of loans and credits. In this case, loans and credits are repaid with money from subsequent loans and credits. This method is used to even better conceal the criminal origin of funds flowing to banks as repayment of refinancing loans and credits,
- loans and credits repaid by guarantors. In this variant, the credit or loan is repaid with funds from illegal sources not by the borrower, but by the guarantors,

- credits and loans granted by financial institutions located outside Poland. A resident takes out a credit or loan from a credit institution abroad and then repays the instalments with the profits from illegal activities. The money transferred to Poland on this account comes from a definitely legal source.

378. *"Pass-through account".* This method consisting in crediting an account using transfers coming mainly from one source in order to immediately transfer the thus obtained funds to another account. For reasons related to the speed of funds transfer, accounts kept with one bank to which electronic access has been established via the Internet, or services enabling the transfer of funds in real time between accounts kept with different banks are often used.

379. Purchase and sale of *fixed assets*. The money laundering method includes three basic variants:

(1) the buyer purchases fixed assets from the seller at a specified price. Then the buyer sells them back to the seller at a price higher than their purchase price. In this way, "dirty money" with a value corresponding to the difference between the values of the two transactions has been introduced into financial circulation;

(2) the buyer purchases fixed assets from the seller at a price much lower than their value. At the same time, the buyer sells the seller other fixed assets of the same type and with similar parameters, but for a much higher price. These two transactions practically did not change the proprietorship of both trading partners in terms of the amount and type of assets owned. However, the flow of money accompanying both transactions enabled the legalisation of "dirty money" with a value equal to the difference between the values of the two transactions. Money laundering in the trade in fixed assets may become more complicated where other types of transactions are combined with the purchase and sale of fixed assets. For example:

   (a) the buyer purchases real estate at a price corresponding to its market price, and then contributes it in-kind to a commercial partnership or company, inflating the value of this real estate and, as a result, also the value of the company itself, and then sells its shares in the said company to a bogus investor or investors,

   (b) the buyer purchases fixed assets at an inflated price, the payment is transferred to the seller partly by the bank that granted the buyer a loan, and the buyer repays the loan instalments with "dirty money".

380. The money laundering method using trade in fixed assets has the following characteristics: personal, organisational or financial links between the buyer and the seller, overstatement or understatement of the value of fixed assets being traded, purchase and sale transactions of the same fixed assets in a relatively short time.

381. It should be noted that not only businesses, but also natural persons who do not run a business may engage in money laundering through the purchase and sale of fixed assets (e.g. real estate, cars).

Example

The General Inspector of Financial Information, in consultation with the prosecutor's office, analysed financial flows related to the laundering of money obtained from fraudulent real estate

restitution. Interrelated persons participated in obtaining under false pretences the return of high-value real estate by misleading former owners and legal successors as to the real value of the real estate and persuading them to sell the debt below its actual value. The GIFI analysed transactions carried out within one year. The findings made by the Polish FIU showed that many transactions were carried out between the accounts of persons involved in this illegal operation. Cash payments were made to the analysed accounts, the accounts were credited with funds related to the purchase of real estate from third parties, and some of the funds came from the City Hall and the bailiff. The funds transferred to the bank accounts of the persons involved in the case were withdrawn in cash, invested in securities, used to purchase real estate or transferred abroad. Reciprocal donations were also made, to be later cancelled and to return the funds involved. Such transactions were intended to make it difficult to detect links with criminal activity and to make it more difficult for potential victims to pursue claims for repayment of funds or restitution of the real estate. Moreover, the probable purpose of the large number of cash transactions and transfers of funds abroad was to hide the funds and blur their source of origin. The GIFI blocked a total of approx. PLN 4.3 million in the accounts held by those participating in this illegal operation and submitted two notifications on the suspicion of committing the offence referred to in Article 299 Penal Code to the prosecutor's office.

382. *Family transactions.* Family transactions, as a method of money laundering, mean activities carried out between natural persons with any degree of kinship or affinity, as well as legal and natural persons, and only between legal persons (assuming the existence of kinship between natural persons that are members of the bodies of these legal entities), where the circumstances of the assets disposition show that the transferred assets come from an undisclosed or illegal source, and the transfer of ownership itself is intended to conceal the origin of the aforementioned assets. Family transactions may be simple transactions, i.e. transfers of funds between bank accounts, e.g. as a gift, loan, loan return, or may be only one of the elements of complex financial transactions, e.g. some of transactions between businesses run by spouses, made as payment for a service or goods. The largest scale – in terms of the value of transactions – of the described method of money laundering can be noted where there is kinship between members of the governing bodies of commercial partnerships and companies. This applies in particular to transactions between subsidiaries. Such a situation may occur where the president of the management board acts to the detriment of the company, as a result of which part of the funds will be transferred to the account of a subsidiary in which one of the management board members is, for example, a person related to the president of the parent company.

383. *Money laundering using accounts intended for the same person.* The name of this method is descriptive and its purpose is to indicate the possibility of money laundering by a specific person (persons) through accounts kept for that person. When laundering money using this method, other methods may also be used, but practice shows that most often we are dealing in this case with structuring, i.e. transactions in amounts below the threshold requiring registration. This method is characterised mainly by laundering money with the use of accounts held by the launderer. It should be clarified at this point that the term "accounts held by the launderer" should be understood as accounts kept both for natural persons (e.g. spouses) and legal persons (e.g. an account kept for a company belonging to the launderer). Money laundering, using accounts held by the launderer, can be carried out both through very simple

transactions and more complex ones, constituting a specific "path" of various transactions. Typical cases of money laundering using the method concerned include:

- cash deposits and cash withdrawals (to and from the same account), most often in amounts below the threshold requiring registration,
- opening term deposits (preceded by a cash deposit),
- making transactions using the following patters: cash deposit – transfer/transfers – cash withdrawal (these transactions are often accompanied by structuring deposits and withdrawals),
- making transactions using the following pattern: cash deposit (structuring deposits) – transfer/transfers and/or currency conversions – transfers to other accounts, e.g. payments for goods, as well as making other payments typical of "normal" business activity, including payments to the Social Insurance Institution (ZUS) and the Tax Office.

384. It should also be added that in the third and fourth cases described, the payments initiating the money laundering "path" are made to the launderer's personal accounts, not to company accounts. As for transaction amounts involved in this method, apart from the previously mentioned amounts below the threshold requiring registration, it is difficult to discern any methodology of the launderer's operation. It follows from the GIFI's experience that, for example, term deposits were made for amounts ranging from several dozen to several hundred thousand zlotys. As for transfers between accounts, they were not always for the same amounts that were deposited in cash. A similar remark can be made as regards cash withdrawals (also by cheques and from ATMs), whose amount does not have to be the same as that of particular transfers between accounts. An even more complicated example illustrates the situation described in the fourth of the above cases where the funds, after passing the "path" of various transactions, are transferred to the company account and are allocated for payments to trading partners (entities not involved in money laundering) or to settle the tax liabilities of a given entity. In this case, the transfer amounts can practically no longer be linked to the amounts deposited in cash at the beginning of the "path".

385. *Money laundering related to the change of the form of assets.* In the case of this method of money laundering, it should be noted that the list of methods of changing the form of assets to commit a criminal act is non-exhaustive. Based on the experience of the Polish FIU, besides the methods described herein, i.e. purchase/sale of fixed assets, virtual assets and foreign exchange, several other methods of implementing these activities should also be mentioned. These include, for example, the exchange of illegal funds for precious stones, gold, cheques or treasury bills. Trade in precious stones and gold is often used by criminals and organised criminal groups. Gold and precious stones are an extremely attractive means of money laundering. They provide organised criminal groups with a mechanism for transforming illicit cash into a stable and, above all, anonymous form of asset in order to take or reinvest profits from their activities. An example of one of the indicated methods is presented below.

Example

Trade in precious metals of unknown origin. The case in question was initiated by a notification from an obligated institution sent to the GIFI. The notification concerned the purchase of

precious metals, mainly gold and silver, by a married couple running a currency exchange office and a pawnshop. Precious metals were then sold to two foreign entities dealing with their processing. These persons claimed that gold and silver came from jewellery purchased from many people. However, this information raised doubts as the very high value of transactions would mean that the group of customers would have to be very large. It should be noted that gold and silver jewellery is a popular gift for special occasions and the recipients usually do not sell it without important reasons. Moreover, these persons operated only a few outlets where they purchased precious stones. Their number did not correspond to the significant number of customers selling their jewellery. In the case in question, after the analysis (information obtained from available sources, as well as based on available tax and criminal databases), the GIFI sent a notification to the prosecutor's office and a notification to the customs and tax-control office.

386. It follows from the GIFI's experience that money laundering related to changes in assets is in many cases combined with the use of crypto-assets – virtual currencies. It should be noted that the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* includes the concept of "virtual currency". In the Act, a "virtual currency" is defined as a digital, transferable representation of value that is used as: (1) a means of exchange and/or, (2) a unit of account and/or, (3) a store of value that does not, however, have the status of a legal tender in no jurisdiction and is not issued or guaranteed by any government, and serves the above functions only by agreement within the community using this currency. The above definition indicates directly that virtual currencies are not a legal tender, and, indirectly, that they are not electronic money. However, this does not determine their legal nature or whether the virtual currency is a good, service or property right[180]. *The Act on counteracting money laundering and financing of terrorism* aims to oblige providers of network services related to virtual currencies, i.e. Virtual Asset Service Providers (VASPs)[181] to monitor transactions, collect data, report abuses to supervisory authorities, and provide digital traces.

387. On 31 October 2021, new regulations came into force regarding the operation of entities from the cryptocurrency industry – cryptocurrency trading facilities and cryptocurrency exchanges. The amended *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* provides for the obligation to obtain an entry in the register of virtual currency service providers[182] for entities providing services: exchange between virtual currencies and legal tenders, exchange between virtual currencies, brokerage in the exchange referred to above, maintaining accounts enabling authorised persons to use virtual currency units, including conducting their exchange transactions.

[180] *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937* (MiCA – Markets in Crypto Assets) was published in June 2023. The Regulation identifies the following three categories of crypto-assets: asset-referenced tokens; electronic money tokens (e-money tokens); crypto-assets other than asset-referenced tokens and e-money tokens.

[181] The collective name VASP comes from the nomenclature used by the FATF and covers digital currency network service providers that have a special role in the anti-money laundering system.

[182] The register is kept by the Revenue Administration Regional Office in Katowice. Link: https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych

388. It follows from the GIFI's experience that a significant part of information concerning suspicious transactions regarding trading in virtual currencies is transferred to the Polish FIU by banking sector entities.

Example 1

The case was initiated based on information provided to the GIFI by an obligated institution, regarding suspicious financial transactions carried out by a company ("shell company"). Based on an analysis of the company's account record and publicly available information about this company it was established that the company in fact operates as a cryptocurrency exchange. Due to the fact that this entity closed its bank accounts in Poland, but it was still possible to purchase/sell virtual currencies through the entity's website, the GIFI sent a notification to the customs and tax-control office under Article 106(1) of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism. Based on the information received from the customs and tax-control office in response to the GIFI's notification, it was noted that in this very case, the prosecutor's office is investigating the use of the company's accounts to receive funds from phishing. The activities carried out by the prosecutor's office showed that no business activity had ever been conducted at the registered office address indicated by the company. The customs and tax-control office sent a letter to the entity concerned requesting it to provide documents related to its business activity. The letter was returned to the sender (the customs and tax-control office) due to the addressee's failure to respond within the prescribed period. Due to the above, the office submitted a request for an inspection of the company's main trading partner.

Certain activities are still being carried out in the case by the customs and tax-control office and the prosecutor's office.

Example 2

The case was initiated based on a notification sent to the GIFI by an obligated institution, regarding suspicious transactions carried out by a company whose account was credited almost exclusively by natural persons. Then, the funds were transferred to a foreign exchange dealing in cryptocurrencies. Based on an analysis of information regarding the aforementioned company it was found that it was not entered in the register of payment institutions and had personal relationships with the cryptocurrency exchange. At the bank's request, the company provided a trust deed concluded with the cryptocurrency exchange for the safekeeping of funds. Due to the suspicion that the trust deed was an attempt to circumvent the laws on the provision of payment services, the GIFI sent a notification to the Office of the Polish Financial Supervision Authority. Finally, the Polish Financial Supervision Authority entered the entity on the list of public warnings.

389. *Loans and donations.* Among the civil law transactions described in the *Civil Code*, donations and loans are those that are the most frequently used in money laundering. A natural or legal person obtaining profits from illegal undertakings that they wish to legalise communicates with other persons in order to prepare a fictitious loan or donation agreement, and then registers such deeds with the tax office, paying the due tax on civil law transactions. This method is effective because lenders and donors are not obliged to provide reasons for

granting a loan or donation, or to document that they have sufficient funds to complete the transaction. In the case of loans, "dirty money" may be legalised not only through the fictitious transfer of ownership of the funds, but also through the apparent repayment of interest on the loan granted. Pursuant to a loan agreement, the borrower is obliged to repay principal and interest instalments according to an agreed schedule and at a specified interest rate. Therefore, money laundering may take place not only through granting a loan and thus laundering the borrower's profits from illegal undertakings, but also through repaying a fictitious loan with interest, based on which the lender is able to legalise "dirty money". The most common variants of the aforementioned money laundering methods include loans and donations granted by foreign persons and entities, especially by companies registered in "tax havens". When using a *donation* in money laundering, two or more natural persons or businesses agree to make an apparent transaction of transferring ownership of a specific amount corresponding to the value of the "dirty money". A person or entity generating sufficient income to be able to make the aforementioned transaction is sometimes chosen to be the donor. The donee, once they have legal ownership of these funds, may introduce them into financial circulation, e.g. deposit them at their own discretion in a bank or investment account. Sometimes money laundering does not end with just one donation transaction, but takes the form of a long chain of transactions in which the donee in the first transaction is the donor in the second one. In this way, criminals try to hide the original, criminal source of money. This method of money laundering is largely related to other, indirect transactions/activities of persons participating in this crime (other variations of this method) and is often part of the process related to the discussed illegal practice, that in this case is ultimately intended to conceal the source of illicit funds. Examples illustrating this method are provided below.

Example

The case was initiated by a notification sent by an obligated institution to the GIFI. After the notification was submitted, the GIFI received information from a foreign FIU that a person related to the companies described by the obligated institution was a PEP[183] *and was convicted of corruption in their home country. Investigative authorities in country (A) of the foreign FIU established that this person used money from obtained financial benefits to purchase real estate in Poland. Just before sending a request from abroad to seize the real estate, it was sold to other citizens of requesting country A. Country A requested for: (1) establishing the details regarding the further 'path' of the transfer of the funds from the sale of the real estate, (2) blocking the bank accounts linked to the aforementioned person (PEP). Moreover, the Polish FIU asked the prosecutor's office to provide information on the implementation of the request for international legal assistance. It also analysed the records of the accounts and links between particular persons. It was found that a group of people, citizens of the requesting country, had owned personally and financially related companies in Poland for several years. According to the available information, on one day, person (B), having family ties with the PEP, transferred funds in connection with a purchase/sale transaction regarding real estate in Poland. At the same time, the funds held by person B came from a purported loan (transaction title) granted by another person (C), also personally related to the aforementioned PEP. In the next step, part of the funds were withdrawn in cash and the remaining amount was transferred abroad. Due to the suspicion of a fictitious sale of real estate between persons with business relationships in*

[183] Politically Exposed Persons

order to prevent its seizure by the prosecutor's office, the GIFI sent a notification to the prosecutor's office.

390. *Leasing and factoring agreements.* Money laundering using leasing agreements should be analysed in terms of three possible ways of committing this offence, i.e. (1) at the moment of handing the item over to the user, (2) at the moment of recognising that assets from illegal or undisclosed sources will be introduced into financial circulation at the time of payment of leasing instalments, and (3) at the moment of recognising that assets from illegal or undisclosed sources will be introduced into financial circulation at the time the item is purchased by the user. We will be dealing with money laundering either when legal tenders or the item are introduced into circulation, depending on which of the above options will be recognised as the moment of money (property) laundering. Referring to the first of the aforementioned options, i.e. recognising that laundering using leasing contracts takes place upon the transfer of possession of the item leased to the user, it is difficult to resist the impression that such reasoning could lead to absurdity. If we consider the transfer of possession of the item as the introduction of assets from an illegal source into financial circulation, we would come to the conclusion that it is the financing party that is the launderer. Of course, such a model is theoretically possible. In practice, it is unlikely and qualifies rather as fencing of stolen goods (Article 291 of the *Penal Code*). The same applies to the third (3) of the above options, i.e. recognising that the introduction of assets from illegal sources into financial circulation occurs at the time of purchase of the item by the user. Therefore, what remains is the second (2) of the above options, i.e. recognising that assets from illegal or undisclosed sources are introduced into financial circulation at the time of paying leasing instalments. It should also be mentioned that leasing, as an economic phenomenon, can be used by launderers using the so-called goods smurfing. In this case a luxury item is purchased by a person related to a criminal group. An item may also be purchased by a random person recruited to perform a specific activity ("straw man"). This person legitimises the purchase of, for example, an expensive car by providing their personal data. Then the item is sold to a leasing company controlled by a criminal group, whereby the item is leased again to the person who sold it or to another person recruited for this purpose. Factoring is0000000 slightly different from leasing. Its main purpose in not purchasing fixed assets, but preventing payment backlogs. By using factoring, a company can immediately obtain receivables under issued invoices to have funds for current operations or any other purposes. A factoring agreement is a commonly used form of settling receivables for goods or services and financing transactions. It belongs to unnamed contracts, i.e. contracts not regulated in positive law. It is a bilateral agreement between the factoring party and the factor. For such an agreement to be concluded, the presence of a third entity – the debtor – is necessary. As part of a factoring agreement, the factor purchases receivables (usually short-term ones) due to the factoring party from the debtor, and commits to provide specific services in exchange for the transfer of receivables, purchase of specific services and payment of a commission and interest.

Example

Two notifications were sent to the General Inspector of Financial Information from various obligated institutions, regarding a company conducting business consisting in wholesale of other household products. During the analysis of the received information, checks relating to the indicated company were carried out (in the GIFI's databases) and data regarding additional three bank accounts maintained for the aforementioned company was obtained. In

connection with obtaining additional information, the banks maintaining accounts for the company were requested to provide the records of the company's accounts. At the same time, an Internet search for information regarding the entity was carried out (an analysis of the website of the company that advertised itself there as a direct importer of products from China and Indonesia). Suspicions in this case were raised by: the pattern of transactions, transfers between companies, the amounts of transfers made ('round' transaction amounts), and the identified personal and capital connections. The analysis of the case showed that the company, under a reverse factoring[184] agreement concluded with a factoring company, settled liabilities with six trading partners (entities with personal, transactional and capital connections with the company) that, once they had received the funds (usually on the day of their receipt), ordered transfers to the company concerned, as "refund of an advance payment" or "refund of a deposit". At the same time, the company transferred a significant part of the thus obtained funds to a certain entity (financial broker/online currency exchange platform). A data analysis showed that no transactions confirming the import of goods from Asia were carried out, and the invoices based on which the payments were made raised doubts as to their credibility. Moreover, the activities of some of the company's trading partners were followed by one of the prosecutor's offices in connection with ongoing proceedings regarding an offence under Article 271a(1) of the Penal Code (fraudulent misrepresentation of a document in the form of an invoice). Having collected materials in the case concerned, a few weeks after it had received the notifications from the obligated institutions, the GIFI forwarded a notification to the locally competent prosecutor's office, that was then sent to the prosecutor's office supervising the proceedings conducted in relation to, among others, the financial broker/online currency exchange platform.

391. *Currency exchange transactions (exchange of foreign exchange values).* Currency exchange transactions often involve small amounts and are not subject to registration. They can also be made in larger amounts, but usually by recruited persons in several different currency exchange offices or bank branches. In this way, the origin of the money exchanged is documented with receipts confirming that the aforementioned transactions have been carried out. Since such documents are, however, poor evidence confirming the legal origin of the aforementioned values, this method is usually combined with other money laundering methods.

392. *Trading in stocks and shares*. This method involves purchasing shares at a "normal" price in order to resell them at a higher one. The last transaction may (but does not have to) be accompanied by cash flow. Its main purpose is to legalise the ownership of the investor selling shares. In this case, the investor may be an entity selling shares or stocks on the secondary market or the joint-stock company itself (issuing additional shares). Purchasing/selling shares at a lower price is another option of this method under which the seller receives, besides the official payment, also a less official compensation for the difference between the market price and the transaction price, while the buyer holds shares or stocks whose value is similar to the profits from illegal activities subject to laundering. These shares or stocks can then be safely sold further, thus obtaining legalised funds. The above options of this method are often combined and may include the following stages:

[184] Reverse factoring involves financing invoices from suppliers, i.e. cost invoices. In this case, invoices for purchases or services are most often financed. This solution allows for splitting cost invoices into instalments.

- the first stage consists in the purchase of shares from a large number of their holders in several dozen transactions. The share purchase price, according to the purchase and sale agreements, was close to the nominal price. In fact, the price per share paid by the broker was much higher and was several or a dozen or so times the price specified in the sale and purchase agreement,
- the second stage consists in the sale of the purchased shares at a higher price to another, second broker. At this stage, the price is nominally several times higher than the nominal one, but the difference between the actual purchase price at the first stage and the selling price at the second stage is small. This is how a group of "second brokers" is created. The share price at this stage may be equal to the actual purchase price at the first stage,
- at the third stage, a group of "second brokers" sells shares held by them. At this point, there are two ways to dispose of shares:
  - shares are sold to two or three entities that do not resell them. (This leads to the " parking" of the shares purchased at the first stage. As a result, the group organising the purchase of shares, through their resale to subsequent brokers from the group and then to the final buyer, is in possession of "laundered" cash. It should be added that among the types of entities mentioned in the previous stages, there is a network of connections resulting from powers of attorney and authorisations to other people's accounts),
  - the shares are sold in a series of transactions to other buyers not related to the "group".

393. Money laundering through trading in stocks and shares may also involve the purchase of shares for "dirty money" in a company that brings profits just before the dividend payment. In this case, part of the funds spent on the purchase of shares is transferred in "pure form" by the company to the buyer as payment of share in profits. This option of money laundering through trading in stocks and shares can be combined with the "shell company" method, where shares or stocks in a company conducting fictitious business, established to legalise profits from crime, are traded. "Dirty money" invested in the company to purchase fixed assets increases its value, thus enabling the sale of its shares at a sufficiently high price.

394. Another option of the money laundering method concerned involves the purchase of shares in a Polish company by a foreign entity. Shares are purchased by a non-resident usually at a price higher than their market price. Money used in these transactions may come from:

- offences committed abroad,
- offences committed in Poland, the profits from which were then transferred abroad.

395. However, the above transactions are not always accompanied by a cash flow. Sometimes contracts for the sale of shares in a Polish company abroad are fictitious and their purpose is to document the origin of the funds used by the seller. In this case, such contracts registered with the tax office are the only documents confirming these transactions. Another option of this money laundering method involves making an in-kind contribution in the form of rights acquired in exchange for part of the shares in the company. The value of the in-kind contribution made by the entity to the company is much higher than the nominal value of the

purchased shares of this company. The surplus of the value of the in-kind contribution over the nominal value of the shares is included in the share premium. The money intended for the purchase of acquired rights contributed in kind may come from crimes committed in Poland and abroad. This means that this share premium profits persons who are the company's current or future shareholders, constituting a form of hidden transfer of value to these persons, i.e. the hidden beneficiaries of the described transaction.

396. It follows from the Polish FIU's experience that money launderers often resort to the "cross-border money transfer" method that involves the physical or non-physical transfer of funds across the country's borders for their further transfer or investment. This method is often combined with some of the aforementioned methods. The main purpose of this method is to isolate funds as much as possible from their criminal source, primarily by removing them from the jurisdiction competent for the predicate offence.
The following types of cross-border cash transfer can be identified:

- *cash transfer* using "cash couriers" – physical transfer of money seems to be the simplest mutation of the method concerned. It does not require direct contact with employees of financial institutions or using the services of entities operating alternative cash transfer systems. In the case of a one-time transport of money, this option seems to be cheaper than the others, because it does not involve paying fees or commissions required by middlemen. Due to Poland's accession to the Schengen Agreement and waiving border controls with other EU countries on 21 December 2007, it is now possible to freely transport profits from crime or profits that may be used to finance terrorism between Poland and other areas of the European Union. This poses a major risk relating to transport of illicit proceeds from Poland to other European Union Member States and the other way round. There are a number of ways to hide cash to prevent it from being detected when crossing the border. Based on the experience of various countries, it can be concluded that the methods used in this case are similar to those used to smuggle drugs. It should also be noted that money is transported not only in the form of banknotes or coins (especially ones minted in precious metals such as gold or platinum), but also in a form corresponding to the development of financial market products, including cheques, electronic payment instruments (including prepaid cards),
- *transfer of funds using a bank account* [cross-border transfer[185]],
- *alternative money transfers* – cash transfer through companies offering services in this area:
  - non-bank payment services – money laundering or financing of terrorism can take place also with the use of payment services offered by entities operating alternative remittance systems (ARS), including through domestic payment institutions, payment service offices, small payment institutions, as well as agents of foreign entities such as Western Union or MoneyGram. This type of cross-border transfer of funds is used by, among others, non-residents in order to transfer profits (often originating from the shadow economy) obtained in Poland to their

[185] A method described above – "cross-border transfers" (fund transfers via a bank account).

home countries due to the so far less restrictive rules for identifying the parties to the transaction, and, in particular, the payee,

– informal money transfer systems – besides legally operating companies providing money order services, middlemen that do not conduct officially registered activities in this area may also be used to transfer funds across borders. In this case, their services are most often referred to as "underground" or "informal banking". Such systems of transferring funds often have names derived from the languages of the ethnic groups that use them most often, e.g. "hawala", "hundi", "da shu gong si" (or "fei chien" or "fei quian") or "padala". Such systems are based on several fundamental principles: trust in middlemen (called e.g. "hawaladar" or "hundiwal") resulting from, among others, the principle of clan and family responsibility for the received funds, using codes assigned to particular transactions in contacts with the principal and the beneficiary, minimising physical transfers of money by using commodity or invoice settlements between middlemen (i.e. a middleman receiving funds in one country and a middleman who disburses them in another country).

397. Besides the money laundering methods (indicated in Chart 5) whose percentage was the largest in 2019-2022, other methods (often related to the aforementioned ones) and practical examples of cases arising from the activities carried out by the GIFI should also be mentioned.

398. It should be noted that 2020 was the year when the COVID-19 pandemic began. During this period, there was a significant change in the activities of criminals/criminal groups resulting from the specific changes caused by the pandemic as regards financial transactions, i.e. a significant increase in online purchases/sales/financial transactions by natural persons and businesses, as well as the methods/types of offences committed by natural persons and organised criminal groups.

399. In 2020, a number of analyses of the impact of the COVID-19 pandemic on changes in the methods of money laundering and financing of terrorism were carried out. Those analyses were performed, among others, by the FATF ("COVID-19 related Money Laundering and Terrorist Financing – Risk and Policy Responses"[186] from May 2020), MONEYVAL ("Money Laundering and Terrorism Financing trends in MONEYVAL jurisdictions during the COVID-19 crisis"[187] from September 2020), EUROPOL ("How COVID-19 related crime infected Europe during 2020"[188] from November 2020) and the Council of Europe ("COVID-19 Vaccine fraud: Operational response and preparedness" from April 2021).

400. The informational included in these documents focused, among others, on areas where the pandemic had increased the risks related to money laundering and financing of terrorism. It should be noted that the COVID-19 pandemic has increased the assistance provided by particular governments to mitigate the effects of the pandemic (e.g. social aid initiatives or tax relief for particular industries affected by the crisis caused by the virus). The indicated actions of particular countries in the initial phase of the pandemic were abused by criminals and organised criminal groups. These reports describe particular types of offences and the methods

[186] https://www.fatf-gafi.org/publications/covid-19/covid-19.html?hf=10&b=0&s=desc(fatf_releasedate)
[187]https://www.coe.int/en/web/moneyval/-/covid-19-money-laundering-and-terrorism-financing-trends
[188]https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

of committing them (some of these offences emerged in connection with the COVID-19 pandemic). The information contained in the reports refers to four main areas of offences committed, i.e.: (1) obtaining funds by deception and fraud, (2) cybercrime, (3) corruption (4) other offences, e.g. human trafficking, drug trafficking, exploitation of minors on the Internet, organised crime against property. It should be noted that in the case of certain offences, e.g. trafficking in drugs and psychotropic substances or exploitation of minors on the Internet, the specific characteristics of the methods of their committing changed. This was due to the impossibility of movement of natural persons in the initial phase of the pandemic (for example, trafficking in drugs and psychotropic substances moved to the Internet – online transactions, so did offences related to the exploitation of minors).

401. In the case of activities related to counteracting crime at the EU level, attention should be paid to the organised, coordinated action of EU Member States supported by EUROPOL and OLAF called *'Operation Shield'*[189], which resulted in arresting 667 individuals involved in offences related to, among others, fraud in the sale of medical equipment, pharmaceuticals or COVID-19 tests. The details of this operation are described below.

Operation Shield

In 2020, EUROPOL coordinated Operation Shield aimed at combating trafficking in counterfeit medicines, medical products and doping substances. The operation was led by Finland, France, Greece and Italy and involved law enforcement authorities from 27 countries (19 EU Member States and 8 third-party countries), the European Anti-Fraud Office (OLAF), the Pharmaceutical Security Institute and the private sector. The operation took place between March and September 2020. During the operation, law enforcement officers dismantled 25 criminal groups, arrested 667 suspects and seized large amounts of medicines and medical devices. As for the latter, almost 33 million face masks, COVID-19 tests and diagnosis kits were seized. The services also seized 8 tonnes of medical raw materials, chemicals and antivirals as well as 70,000 litres of hygiene sanitisers.

402. In the case of fraud related to medical products, the actions taken as part of the INTERPOL operation called PANGEA XIII[190] that took place in 2020 should also be mentioned. As part of this coordinated operation, the services seized counterfeit face masks and counterfeit medical supplies.

Operation PANGEA XIII

The Police, customs authorities and health care services from 90 countries took part in PANGEA XIII – an action against the illicit online sale of medicines and medical products. Law enforcement agencies taking part in Operation Pangea found 2,000 online links advertising items related to COVID-19. Of these, counterfeit surgical masks were the medical device most commonly sold online, accounting for around 600 cases during the week of action. As part of this operation, more than 34,000 counterfeit and substandard masks, "corona sprays" or "coronavirus medicines" were seized.

[189]'Operation SHIELD', https://www.europol.europa.eu/newsroom/news/medicines-and-doping-substances-worth-%E2%82%AC73-million-seized-in-europe-wide-operation

[190]https://www.interpol.int/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19

403. The spreading COVID-19 pandemic resulted in a number of actions aimed at supporting the Polish economy and the private sector, undertaken by the Government of the Republic of Poland, e.g. by introducing the so-called anti-crisis shield, and with respect to the *Act on counteracting money laundering and financing of terrorism* – by postponing the final deadline for registration of companies established before 13 October 2019 in the Central Register of Beneficial Owners until 13 July 2020. Targeted social actions and measures were also taken to limit the spread of the epidemic in Poland, e.g. by restricting the movement of people, both within Poland and outside its borders. Most public administration institutions worked from home. Similar principles were also introduced by a number of private sector institutions. The aforementioned actions caused criminals to change their *modus operandi*, while taking advantage of the COVID-19 pandemic to expand the scope of criminal acts committed by them.

404. As part of its activities, the Polish FIU noted, as in the case of pan-European experience, similar threats regarding the impact of the COVID-19 pandemic on risks related to money laundering and financing of terrorism. According to available information criminals tried to benefit from the pandemic by, among others, fraudulently raising funds for fake charities, making sales without physically handing over the goods, various types of fraud related to the medical sector, or online sales of counterfeit medicines and medical supplies, such as COVID-19 test kits and personal protective equipment. In some cases, criminals also pretended to be officers of the Police or other services, including health care services, to get to their victims' flats or obtain access to their personal data, details of their bank accounts and other information. As part of its activities, the Polish FIU also identified a number of offences within broadly understood cybercrime. To install malware on personal computers or mobile devices, criminals took advantage of social concerns regarding COVID-19, by impersonating various types of public administration institutions, energy suppliers, or other entities, institutions or international organisations. Phishing attempts, involving creating fake emails from the World Health Organisation and installing malware on mobile applications by criminals, were reported. Criminals also pretended to be health care providers, offering treatment or promising to provide funds to help in emergencies requiring medical intervention.

405. The Polish FIU recorded *counterfeiting of goods, i.e. medicines and medical supplies.* The recorded abuses resulted mainly from the high demand for the aforementioned medical supplies. In 2020, there was an increase in the scale of fraud in the trade in/sales of medical supplies, personal protective equipment and pharmaceutical products. In such cases, criminals claimed to be, for example, employees of companies, charities or international organisations offering face masks, COVID-19 test kits and other medical devices, and demanded, as part of the sales contract, the purchaser's credit card details for payment or shipping, but never delivered the purchased goods.

406. In some cases, victims were asked to pay in advance by bank transfer and then the goods were sent to different locations to be collected, only to be informed later that no such arrangements had been made. In similar fraud cases, goods were delivered to the consumer, but turned out to be counterfeit or worthless. In the cases it conducted, the Polish FIU identified a number of offences related to, among others, fraud involving offering protective masks or obtaining funds by deception by entities using, for example, the so-called shields.

Example

(fraud related to offering protective masks, identified in trade therein with Asian countries)

The case was initiated by a notification from an obligated institution regarding obtaining funds by deception from a number of natural persons in connection with offering protective masks. The EUR and PLN accounts of a Polish company A were credited with funds from natural persons and businesses. The transaction titles indicated payments for ordered protective masks. The total amount of funds that credited the said accounts exceeded several million PLN within 4 months. Some of the funds were transferred to another Polish company B, then transferred to China and withdrawn in cash abroad. The bank maintaining the accounts of company A began to receive an increasing number of messages from the banks originating the transactions requesting it to refund the funds, as well as complaints about the ordered transactions that could suggest fraud. A number of negative reports on transactions concluded with the company concerned were found in generally available databases. It could be concluded from the comments that a large number of people had been defrauded when purchasing protective face masks through the website that operated only for a specific time needed to commit the criminal act. The analysed company A was not registered for VAT purposes and did not submit any tax returns to the Polish tax authorities throughout the period of its operation. The Polish FIU collected information which showed that company A and its sole shareholder and at the same time its CEO had been monitored by law enforcement authorities in connection with the committed fraud. Based on this information the GIFI blocked a significant part of crime proceeds on the accounts of company A and sent a notification to the competent prosecutor's office.

407. *Investing illicit funds in real estate.* In times of economic downturn caused by the pandemic, criminals invested, among others, in real estate or businesses at risk of bankruptcy, that were then used to generate cash and conceal illicit proceeds, or to carry out corporate bankruptcy proceedings to conceal the origin of illicit funds.

408. Other criminal activities on financial markets during the COVID-19 pandemic included (1) introducing illicit cash into the financial system by criminals by offering new ways of restructuring loans and credit lines on the financial market, (2) blending of illicit cash with legal assets in connection with an increase in the amount of cash withdrawals, liquidation of stock portfolios and an increase in investment in gold bullion during the pandemic, (3) an increase in the value of mobile transactions on the market caused by the closure of branches and offices of financial institutions (or their operation for a limited time) made criminals and organised criminal groups interested in the alternative system, as a result of which they changed their *modus operandi* (fraud/obtaining funds by deception in the mobile transaction sector).

409. Organised criminal groups could take advantage of the COVID-19 pandemic period to raise or transfer funds, among others, through illegal activities, fundraising under the guise of actions aimed at counteracting the effects of COVID-19 pandemic, and criminal activities in the Darknet.

410. The Darknet (dark web) is a virtual space where almost anything can be bought. The Darknet is an encrypted part of the Internet that contains online content that is not indexed by conventional search engines. Its first structure was developed by the US Naval Research Laboratory in the mid-1990s as an anonymous and encrypted network to facilitate communication between American spies. This project was, however, abandoned. In 2002, a

group of IT specialists revived this project by creating a browser for anonymous communication called The Onion Router (TOR). Buyers and sellers in this network are anonymous, which is why the Darknet is used on a large scale by criminals and those who want to avoid, for example, tax liabilities. Criminals develop new, creative ways to launder money from their illegal activities. The network concerned includes products that are considered illegal, such as weapons or drugs. These opportunities are used by criminals and terrorists. Illegal activities carried out on the Darknet include trafficking in human organs or counterfeit money. Other prohibited products sold there include illegal books, counterfeit ID cards and fixed sports matches. The Darknet includes not only online stores, but also fora and blogs dedicated to questionable topics. Users can find there, among others, Orthodox blogs or websites that incite violence, websites with child pornography and information that, for the good of citizens, could not be made available on the open Internet or in mainstream media. Many government institutions are involved in the fight against illegal transactions made on the Darknet, including EUROPOL[191].

Example

In November 2021, police forces across the world arrested 150 alleged suspects involved in buying or selling illicit goods on the dark web as part of a coordinated international operation involving nine countries.[192]. More than EUR 26.7 million (USD 31 million) in cash and virtual currencies, as well as 234 kg of drugs and 45 firearms were seized in this operation. The seized drugs included 152 kg of amphetamine, 27 kg of opioids and over 25,000 ecstasy pills. This operation, known as Dark HunTOR, was composed of a series of separate but complementary actions in Australia, Bulgaria, France, Germany, Italy, the Netherlands, Switzerland, the United Kingdom and the United States, with coordination efforts led by EUROPOL and EUROJUST[193]. Operation Dark HunTOR was initiated in the first phase with arresting by German authorities the alleged operator of DarkMarket (the world's largest illegal marketplace on the Darknet) and closing down this marketplace. The criminal infrastructure was also seized, providing investigators with a lot of information on and evidence of offences committed on the DarkMarket. At the same time, EUROPOL's European Cybercrime Centre (EC3) identified key targets/individuals operating on the DarkMarket. As a result, 150 vendors and buyers who engaged in tens of thousands of sales of illicit goods were arrested across Europe and the United States. A number of these suspects were considered as High-Value Targets by EUROPOL. These arrests took place in the United States (65), Germany (47), the United Kingdom (24), Italy (4), the Netherlands (4), France (3), Switzerland (2) and Bulgaria (1). A number of investigations are still ongoing to identify additional individuals behind dark

[191] European Union Agency for Law Enforcement Cooperation – European Union police agency based in The Hague

[192]https://www.europol.europa.eu/media-press/newsroom/news/150-arrested-in-dark-web-drug-bust-police-seize-%E2%82%AC26-million

[193] European Union Agency for Criminal Justice Cooperation – an EU agency prosecuting organised cross-border crime

web accounts. In the framework of this operation, the Italian authorities also shut down the DeepSea and Berlusconi dark web marketplaces, where a total of over 100,000 announcements of illegal products were recorded. Four administrators of the aforementioned marketplaces were also arrested and EUR 3.6 million in cryptocurrencies was seized.

411. Based on the presented Polish and European experiences regarding new types of threats arising from the COVID-19 pandemic, it needs to be concluded that Europe is facing increasingly complex threats, and criminal groups are taking advantage of digital and technological transformation, as well as the mobility resulting from globalisation. Nowadays, the boundaries between the physical and digital worlds are blurring. The COVID-19 crisis exposed the serious and organised crime landscape, as criminals quickly took advantage of the crisis by adapting their *modus operandi* or developing new criminal activities.

6. THREATS RELATED TO TERRORISM FINANCING

6.1. THREAT OF TERRORISM

412. According to the Global Terrorism Index 2022 report (data for 2021[194]) initial predictions that the COVID-19 pandemic will have a profound impact on the development of terrorism in some regions of the world have not come true. Based on current data, it seems that the pandemic had a relatively minor impact on increasing the rate of growth of terrorist activities, both in 2020 and 2021. In the data for 2022 of the Global Terrorism Index 2023 report[195], the COVID-19 pandemic was no longer included as an important factor affecting the rate of growth of terrorist activities.

413. This limited impact was due to the restrictions introduced in many countries on freedom of movement, restrictions on public gatherings, travel and other forms of interacting with other people for health reasons. Social dissatisfaction was channelled into dissatisfaction with the introduction of lockdowns or the need to undergo mandatory vaccinations. However, extremist groups tried to use the secondary effects of the pandemic, such as a sense of social isolation, increased activity on social media, reluctance to get vaccinated, and dissatisfaction with the economic effects of the introduced lockdowns, for their own purposes. Extremist groups reached out to societies with a message combining health care issues with ideological propaganda to enhance social dissatisfaction and deepen disappointment with the actions of state authorities.

414. According to the aforementioned Global Terrorism Index 2021 report, it was expected in the longer term that the pandemic and its social and economic consequences may increase the likelihood of serious terrorist threats due to, among others, the increased role of the Internet in interpersonal relationships. Since the beginning of the pandemic, the role of online contacts and the role of social media have increased. This shift in interpersonal interactions from typically physical contact towards virtual contact is exploited by extremist and terrorist groups. Due to pandemic restrictions, people have been spending more and more time online, which has opened up an opportunity to spread various conspiracy theories and disinformation. By using the Internet, it is easier for extremist and terrorist groups to undermine trust in governments and gain greater support for the ideology they promote. Using available online tools, various fora, chats and social media, it is easier to fuel racism, anti-migrant sentiments, anti-Semitism, Islamophobia, xenophobia or hate speech. The Internet and social media have become factors that play an increasingly important role in radicalisation and spreading terrorist propaganda.

415. International terrorism constitutes one of the most serious contemporary threats to global security. Countries and regions struggling with disrespecting democracy, human rights and the free market economy are particularly at risk of terrorism. Terrorist attacks are carried out also in developed Western countries. Strong separatist tendencies as well as national, religious, social and racial divisions largely contribute to the development of terrorism. The scale of this phenomenon often goes beyond the borders of particular countries or regions,

[194] https://www.visionofhumanity.org/maps/global-terrorism-index/#/, access on 17.06.2022
[195] Ibidem, access on 17.04.2023

becoming, like Al Qaeda and ISIS, a global threat. Due to the complexity of the problem, terrorism is becoming an inherent element of international politics in the foreseeable future.

416. Data from the Global Terrorism Index 2021 and Global Terrorism Index 2022 reports show a change in the rate of growth of terrorism development in the world. According to an analysis of the collected data terrorist activities are increasingly concentrated in regions and countries suffering from political instability and conflicts, such as the Sahel[196] and Afghanistan. These reports show that conflicts remain the main driver of terrorist activity. Over 88 percent of terrorist attacks carried out in 2022 (97 percent in 2021) took place in countries embroiled in armed conflicts. The Sub-Saharan African region, especially the Sahel, is leading in this ranking. In 2022, 43 percent of all terrorism-related deaths worldwide occurred in the Sahel region (compared to just 1 percent in 2007).

417. A terrorism-related offence is defined in the *Act of 6 June 1997 – Penal Code*. Article 115(20) of this Act provides that a terrorist-related offence is a prohibited act punishable by imprisonment with an upper limit of at least 5 years, committed to:

- seriously intimidate a number of people;
- force a public authority of the Republic of Poland or another state or a body of an international organisation to take or refrain from taking specific actions;
- cause serious disruptions in the political system or economy of the Republic of Poland, another country or an international organisation

- as well as the threat of committing such an act.

418. The Polish system for counteracting terrorist threats is based mainly on the *Act of 10 June 2016 on anti-terrorist activities* (Journal of Laws of 2022, item 2632), that entered into force on 2 July 2016. The systemic approach to terrorist threats applied in this regulation is intended to enable the use of the capacities of all services, bodies and institutions with statutory powers to carry out anti-terrorist activities as well as to streamline and improve the decision-making process at the strategic level. The key purpose of the regulation is to increase the effectiveness of the Polish anti-terrorist system, and thus increase the security of all Polish citizens, by: strengthening the mechanisms for coordinating activities, specifying the tasks and areas of responsibility of particular services and bodies as well as the principles of cooperation between them, ensuring the ability to take effective action where a terrorist-related offence is suspected, including with respect to preparatory proceedings, ensuring response mechanisms adequate to the type of the existing threats, and adapting criminal provisions to new types of terrorist activities.

419. Pursuant to the *Act of 10 June 2016 on anti-terrorist activities*, the leading role in identifying threats related to terrorism is played by the Internal Security Agency, which was reflected, among others, by indicating in this Act the responsibilities of the Head of the Internal Security Agency in preventing terrorist incidents. Pursuant to Article 5(1) of the aforementioned Act, the Head of the Internal Security Agency coordinates analytical and information activities and the exchange of information regarding terrorist-related events between the services. Moreover, pursuant to Article 8(1) of this Act, the Head of the Internal

[196] Sahel, Tropical Sahel – a geographical region in Africa covering the area along the southern edge of the Sahara. The Sahel stretches from Senegal to Eritrea, through Mauritania, Mali, Niger, Chad and Sudan

Security Agency is also responsible for coordinating other services' operational and reconnaissance activities in this area. The Border Guard, the Police as well as other services and institutions support the activities of the Internal Security Agency in this area, among others as part of the Counter-Terrorist Centre of the Internal Security Agency (CAT ABW). Cooperation of the aforementioned services and institutions consists primarily in transferring by officers all information related to incidents and events reportable to the CAT ABW, including direct cooperation in case of recording events indicating a potential terrorist threat. The minister competent for internal affairs is responsible for preparation for taking control over terrorist-related events through planned activities, responding where such events occur and eliminating their effects, including restoring resources used to respond to these events.

420. The terrorist threat level is determined based on the provisions of the *Act of 10 June 2016 on anti-terrorist activities*, that introduced a generally applicable system of alert levels. Regardless of the above, it should be noted that monitoring terrorist threats as well as their analysis and assessment are the tasks of the Interministerial Team for Terrorist Threats[197], chaired by the Minister of the Interior and Administration.

421. According to information available to the National Prosecutor's Office, in 2021, prosecutor's offices conducted 6 (8 in 2020 and 8 in 2019) preparatory proceedings in cases regarding terrorist offences[198]. In 2021, the proceedings in question involved one suspect (compared to 22 in 2020 and 2 in 2019). In three of these proceedings completed in 2021 (9 in 2020 and 1 in 2019), one person was accused (compared to 15 in 2020 and 0 in 2019).

422. The Polish anti-terrorist protection system involves a number of services and institutions. Their participation in the system consists in the implementation of statutory provisions relating to terrorism. These services and institutions include the Ministry of Interior and Administration, Ministry of Foreign Affairs, Internal Security Agency, Intelligence Agency, Military Intelligence Service, Military Counterintelligence Service, Police, State Fire Service, Border Guard, State Protection Service, Military Police, Prosecutor's Office, General Inspector of Financial Information, Customs and Tax Control Service, Government Security Centre, National Security Office.

423. Pursuant to the *Act of 10 June 2016 on anti-terrorist activities*, the Head of the Internal Security Agency is responsible for preventing terrorist-related events. Coordination instruments used to implement activities in the prevention phase include:[199]:

- coordination of analytical and information activities undertaken by secret services and exchange of information provided by the Police, Border Guard, Marshal's Guard, State Protection Service, State Fire Service, National Revenue Administration, Military Police and Government Security Centre, regarding terrorist-related events and data regarding persons referred to in Article 6(1) of the aforementioned Act (including persons undertaking activities for terrorist organisations) by its collecting, processing and analysing,

[197] The Interministerial Team for Terrorist Threats was established pursuant to Order 162 of the Prime Minister of 25 October 2006.
[198] Based on the information provided by the National Prosecutor's Office.
[199] https://www.gov.pl/web/mswia/abw, access on 17.06.2022

- imposing an obligation on the aforementioned services and authorities to provide the Head of the Internal Security Agency with no delay with information obtained to be used to implement anti-terrorist activities, classified in accordance with the catalogue of terrorist-related incidents specified in the *Regulation of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist-related incidents* (Journal of Laws of 2023, item 50),
- keeping, in accordance with the requirements regarding the protection of classified information, a list of persons specified in Article 6(1)(1)-(4) of the aforementioned Act, i.e. persons related to terrorist activities or terrorist organisations,
- providing services, institutions and other public administration bodies within the scope of their competence – as required – with information referred to in the *Regulation of the Minister of the Interior and Administration on the catalogue of terrorist-related incidents* and the information contained in the aforementioned list (also in the form of ongoing analyses of the terrorist threat level),
- providing the President of the Republic of Poland, the Prime Minister, the minister competent for internal affairs, the Minister of National Defence, the minister competent for foreign affairs and the Minister – Coordinator of Special Services with no delay with information that may be relevant to the prevention of terrorist-related events,
- coordination of operational and reconnaissance activities regarding terrorist-related events, undertaken by secret services, the Police, Border Guard, National Revenue Administration and Military Police,
- authorisation to issue recommendations for the aforementioned entities and secret services aimed at eliminating or mitigating the terrorist threat,
- authorisation to obtain, free of charge, access to data and information collected in public registers and records kept by services, institutions, offices and organisational units subordinated to them or supervised by them,
- authorisation to obtain, free of charge, access to recordings from image recording devices located in public buildings, at public roads and in other public places, and receive, free of charge, a copy of the recording,
- appointing, in the event of the introduction of an alert level or a CRP alert level, a coordination staff consisting of representatives designated by secret services, the Police, Border Guard, Marshal's Guard, State Protection Service, State Fire Service, National Revenue Administration, Military Police and the Government Security Centre.

424. One of the main challenges faced by Poland as far as terrorist threats are concerned is its geographical location. Due to the fact that its eastern border is also the border of the Schengen Area, Poland is crossed by routes used to transfer people and goods from the east – the countries of the former USSR and from Central and Southeast Asia. These routes may be used by people related to terrorist groups (including those returning from FTF[200] conflict zones),

[200] foreign terrorist fighters

which entails both a potential threat to the Republic of Poland and to its image on the international stage. In a similar context, the terrorist threat in Poland is affected also by the freedom of travel within the Schengen area. Many EU Member States are struggling with Islamic radicalism (including Belgium, France, Germany), which means that radicals may potentially travel freely around Europe, also to Poland. 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.

425. In 2021, there were mass attempts to illegally cross the state border on its Polish-Belarusian section. Foreigners legally entered the territory of Belarus by air and then attempted to illegally cross the Polish border and enter its territory, supported by the Belarusian state services. Those trying to cross the Polish border illegally include mainly citizens of Iraq, Afghanistan, Syria, Russia, Somalia, Tajikistan, Iran and Türkiye. A total of 39,697 third-country nationals attempting to cross the border illegally on its Polish-Belarusian section were recorded in 2021. It seems that the supporting activities undertaken by the Belarusian services were to destabilise the situation in the Republic of Poland and the European Union. These events were also noticed and described in *EUROPEAN MIGRANT SMUGGLING CENTRE 6th ANNUAL REPORT – 2022*[201]. In 2021, the Polish Border Guard detained/reported 10,458 foreigners crossing the state border contrary to the regulations, compared to 4,156 in 2020.

426. The refugees detained by the Polish services include not only unwarlike economic migrants. On 27 September 2021, the Minister of the Interior and Administration, the Minister of National Defence and the Commander in Chief of the Border Guard held a joint press conference[202]. During the conference, the Head of the Ministry of the Interior and Administration announced that 50 out of the 200 detained refugees were related to terrorist groups, militias, armed formations, the Taliban and the Islamic State. The findings made by the Polish services regarding these 50 people were also presented, including data recovered from their mobile phones. This information was presented by the director of the Department of National Security – spokesman for the minister – coordinator of secret services. Photos from an SD card found by Polish officers on one of the migration routes were also presented. Those photographs showed, among others, meetings of various types of terrorist groups, executions by decapitation, and the bodies of murdered people. One of the Afghan nationals also had a large number of photographs of an arsenal of machine weapons. Photographs of masked people wearing bulletproof vests and carrying weapons were also found. Initial information from the services indicates that the people in the photographs may have operated in informal armed groups. The photographs also showed the migrants' links with Russian territory. One of the Afghans stayed in the Russian Federation for a long time before reaching Poland through Belarus. The collected materials show that he wanted to go to Germany. Other information from the spokesman of the minister – coordinator of secret services shows that cross-examination[203] carried out by allied services confirms the findings of the services responsible for the security of the Republic of Poland: the migrants included dangerous people who should not stay in

[201]https://www.europol.europa.eu/publications-events/publications/european-migrant-smuggling-centre-6th-annual-report-%E2%80%93-2022 access on 17.06.2022
[202] https://niezalezna.pl/412657-terroryzm-tresci-pedofilskie-i-zoofilskie-zaprezentowano-szokujace-ustalenia-polskich-sluzb-ws-migrantow access on 17.06.2022
[203]https://www.tvp.info/56548464/imigranci-powiazani-z-isis-i-boko-haram-stanislaw-zaryn-mowi-o-bialorusi-granicy-i-zagrozeniu-terroryzmem access on 17.06.2022

Poland. Similar problems with illegal migration are faced by Lithuania. The head of the national security committee of the Lithuanian Parliament provided information[204] that further foreigners who came to Lithuania as illegal migrants, to be later found to be related to terrorist organisations or groups, were identified. Some of them have already been deported.

427. In Polish conditions, cases of radicalisation in the Muslim diaspora, both among foreigners living in Poland and Polish citizens professing Islam, are marginal, in spite of free access to propaganda materials of terrorist groups via the Internet, as well as contacts with radicalised followers of Islam abroad.

428. Experience shows that an early response to the first symptoms of radicalisation in society is the most effective method of counteracting extremist and terrorist threats. This goal can be achieved only by ensuring a properly designed and efficiently operating system of preventive measures aimed at people who are susceptible to extremist ideologies. The establishment of a Terrorist Prevention Centre in the structure of the Internal Security Agency (CPT ABW) is one of the systemic activities aimed at accomplishing this goal. The Centre specialises in broadly understood terrorist prevention whose key elements include the dissemination of information about the possible ways of preventing events that may pose a threat to security. The CPT ABW[205] organises tailored training in this area for officers and employees of secret services as well as public administration bodies and other entities. The Centre aims to create a broader prevention mechanism based on the cooperation of all public administration entities and citizens in the process of developing the security culture in Poland. It also aims to accumulate the knowledge and experience of secret services, public institutions, as well as the achievements of universities and scientific institutions to become a forum for the development of cooperation between all entities involved in the security system.

429. To counteract the use of the Internet for terrorist purposes, in April 2021, the EU adopted *Regulation on addressing the dissemination of terrorist content online*[206]. The new provisions have been in force since 7 June 2022. These provisions require online platforms to remove terrorist content from them. Platforms such as Google, Facebook and Twitter have to delete terrorist content within one hour of receipt of the removal order. If they fail to do so, they may pay a penalty of 4 percent of their annual revenue.

430. In case of foreigners (including citizens of EU Member States and their family members) reasonably suspected of conducting terrorist or espionage activities or committing one of these offences, a decision to oblige them to return or to extradite them is made by the minister competent for internal affairs at the request of the Commander in Chief of the Police, the Head of the Internal Security Agency or the Head of the Military Counterintelligence Service. Entrusting powers in this respect to the minister competent for internal affairs is reasonable due to the particular importance of state activities in counteracting terrorism (in other cases provided for by law, the voivodeship governor, the commander of a Border Guard unit or the commander of a Border Guard post are competent to make the aforementioned decisions). Having regard to the potential major threats to state security posed by a person extradited in accordance with the above procedure, it is envisaged that the decision of the

[204] https://www.tvp.info/56548464/imigranci-powiazani-z-isis-i-boko-haram-stanislaw-zaryn-mowi-o-bialorusi-granicy-i-zagrozeniu-terroryzmem/ access on 18.06.2022
[205] https://tpcoe.gov.pl/cpt/o-nas, read on 02.05.2019
[206] https://www.consilium.europa.eu/pl/infographics/terrorist-content-online/ access on 17.06.2022

minister competent for internal affairs will be subject to immediate, compulsory execution. This decision may be appealed against to the Prime Minister as a higher-level authority[207].

431. In order to secure the eastern and northern borders of Poland (being also the border of the Schengen area) against the illegal inflow of migrants, the state border of the Republic of Poland is constantly monitored by foot patrols and using vehicles (passenger cars, off-road passenger cars, motorcycles, quads, and in the winter – also snowmobiles) and aircraft used by the Border Guard (including drones). In sections where the state border runs along watercourses or water reservoirs, vessels are used for this purpose. Due to migration pressure on the Polish-Belarusian border, the Sejm of the Republic of Poland has adopted an Act on the construction of state border security installations. Pursuant to this Act, a physical barrier with installations and accompanying (among others electronic and telecommunications) infrastructure has been constructed. The electronic barrier is intended to protect a section of the border with Belarus of approx. 206 km[208]. The entire system will consist of approx. 3,000 day-night and thermal cameras, 400 km of detection cables and 11 telecommunications containers. The barrier serves to protect the state border and helps prevent illegal migration[209]. A physical barrier made of razor wire has been constructed also on the Polish-Russian border. An electronic barrier has also been installed on this border.

432. Ongoing activities are carried out to provide and exchange information between the Border Guard and the border services of neighbouring countries and FRONTEX. The aforementioned activities consist in the daily mutual exchange of statistical data and the transfer of any information that may be relevant to the protection of the state border or the border traffic flow.

433. The relevant services are constantly taking steps to strengthen migration intelligence with respect to foreigners coming from high-risk countries and staying in the Republic of Poland who are potentially exposed to radicalisation and recruitment to terrorist organisations. Actions are also being taken to enhance the tools enabling ongoing monitoring of the inflow of foreigners to the Republic of Poland, especially from high-risk countries as well as regions and countries affected by conflicts, in order to determine in advance mass migration. Especially after the outbreak of the war in Ukraine, all people entering Poland are identified and verified by the Border Guard. The key issue is to ensure the security of citizens of Poland and European Union countries. As a result of such identification, a terrorist related to the Islamic State was detained when she was trying to cross the Ukrainian-Polish border in a crowd of refugees. The detained woman is probably a citizen of Uzbekistan[210].

434. According to the data of the Border Guard from mid-April 2023, since 24 February, 2022, i.e. from the beginning of Russia's aggression against Ukraine, over 11.15 million refugees from Ukraine, mainly women and children, have crossed the Polish-Ukrainian

[207] Based on the reply of the Ministry of the Interior and Administration of 2 August 2016 to Parliamentary Question No. 3999 (regarding the threat of terrorist attacks in Poland and actions taken at the country borders to ensure internal security as well as the infiltration of people who may pose threat to the security of Poles), available at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.
[208]https://strazgraniczna.pl/pl/aktualnosci/11131,Odebrano-i-uruchomiono-czwarty-odcinek-bariery-elektronicznej-na-granicy-z-Bialo.html access on 18.04.2023
[209] https://orka.sejm.gov.pl › 1657-uzas access on 17.06.2022
[210]https://wgospodarce.pl/informacje/109231-terrorystka-zatrzymana-na-granicy-byla-w-tlumie-uchodzcow access on 17.06.2022

border[211]. The Border Guard also estimates that approx. 9.416 million Ukrainian citizens returned from Poland in the period from 24 February 2022 to 9 April 2023[212].

435. Entities and secret services involved in the Polish anti-terrorist system are required to provide the Counter-Terrorist Centre of the Internal Security Agency with any available information regarding terrorist-related incidents specified in the *Regulation of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist-related incidents*. This Regulation includes, among others, the following categories of classifiable incidents: "departure or planned departure of a person or persons from the territory of the Republic of Poland to an area embroiled in an armed conflict involving terrorist organisations or return from this area". This applies primarily to foreign fighters, including those from EU Member States.

436. According to data contained in the EU Terrorism Situation & Trend Report (Te-Sat 2021), three EU Member States (Austria, France and Germany) reported that a total of 10 jihadist attacks occurred in these countries in 2020. Twelve people were killed and over 47 people were injured in the attacks carried out in these countries. Four jihadist attacks were thwarted in Belgium, France and Germany. In their overall assessment, EU Member States concluded that jihadist terrorism continued to be the EU's greatest terrorist threat. Besides the EU countries, the TE-SAT 2021 report also mentions the United Kingdom and Switzerland. These countries reported a total of 5 jihadist terrorist attacks carried out on their territories (3 and 2 attacks, respectively). Attacks carried out in public places to kill civilians where the most common type of attacks inspired by jihadist ideology in EU countries, Switzerland and the UK. All of the attackers who carried out jihadist terrorist attacks in the EU and the UK were men aged 18 – 33. One of the attacks in Switzerland was probably committed by a woman. All completed jihadist terrorist attacks were committed by individuals acting alone, while at least three thwarted attacks involved multiple suspects. Lone actors or small terrorist groups commit terrorist attacks primarily as a result of being influenced by jihadist propaganda or are ideologically influenced by online content. In addition, jihadist terrorist attacks in Europe were observed to have a motivating effect on other potential terrorist attackers.

437. According to the Global Terrorism Index 2022 (data for 2021), in the West, the number of terrorist attacks had been systematically decreasing over the last three years. Fifty-nine attacks and ten deaths were recorded in the West in 2021, which represents a decrease of 68 and 70 percent, respectively, compared to 2018. According to the aforementioned report, Islamic extremists carried out three terrorist attacks in Europe in 2021. Attacks in the US also dropped to the lowest level since 2015, with only seven attacks recorded in 2021. None of them were attributed to any known terrorist group. In 2021, politically motivated terrorism significantly overtook religiously motivated terrorism, with the latter declining by 82 percent. In the last five years, there have been five times more politically motivated terrorist attacks than religiously motivated ones. Similarities between terrorist attacks driven by ideological reasons are also noticed. Terrorist attracts driven both by far-left and far-right extremist ideologies had similar targets, i.e. politicians and government officials. The analysis of terrorist attacks also shows that most attacks attributed to left-wing or right-wing ideologies are committed by people or groups with no formal affiliation to a recognised organisation. The Islamic State (IS)

[211] https://www.ukrainianinpoland.pl/how-many-ukrainians-have-crossed-the-ukrainian-polish-border-since-the-beginning-of-the-war-current-data-pl/ access on 18.04.2023
[212] Ibidem

remained the deadliest terrorist group in the world, recording the most attacks worldwide in 2021.

438. The Police is engaged in ongoing cooperation with the Counter-Terrorist Centre of the Internal Security Agency in the exchange of information, in accordance with the catalogue of terrorist-related incidents specified in the *Regulation of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist-related incidents*. Activities carried out in particular branches of the Central Investigation Bureau of the Police as regards incidents involving the use of explosive materials and devices in Poland are also coordinated on an ongoing basis. Police officers verify all information that may indicate potential threats posed by terrorist organisations. Their activities include, among others, analysis of terrorist-related events that have occurred and preparation for an effective response to such events.

439. According to the available data, the threat to the security of the Republic of Poland related to religiously motivated terrorist activity remains low. Poland is not in the operational interest of terrorist groups, and the threat related to the activity of people motivated by radical ideology is low. However, given regularly reported terrorist incidents and attacks in Europe, information on FTF departures and returns, propaganda and logistic activity of terrorist groups, as well as factors that may influence the radicalisation or exacerbation of sentiments in the Polish Muslim diaspora are monitored. It must be remembered, however, that Poland was presented in a bad light by the media in the countries from which migrants trying to get through the Polish-Belarusian border to Europe came from. Among the migrants storming the border, Polish services identified people related to terrorist groups, militias, armed formations, the Taliban and the Islamic State. It must also be taken into account that the refugees from Ukraine arriving in Poland after 24 February 2022 could also include some people who may pose a threat to the security of the Republic of Poland. Polish services have detained people suspected of past contacts with the terrorist Islamic State. According to unofficial information, citizens of Tajikistan and Uzbekistan detained at the border are suspected of having contacts with terrorists[213].

440. A major threat to the security of the Republic of Poland in Poland is posed by the possible radicalisation of some representatives of the Muslim diaspora in Poland, which applies both to foreigners living in Poland and to Polish citizens who have converted to Islam. These people may become increasingly radicalised based on propaganda materials of terrorist groups disseminated on the Internet, as well as through contacts with radical followers of Islam living abroad (e.g. by using encrypted messengers, such as Telegram or WhatsApp). In extreme cases, these people, as has been the case several times in Europe recently, may decide on their own to engage in armed jihad as lone actors. Increased religious radicalisation of one of Muslim diasporas in the Republic of Poland has also been recorded. Contacts of members of this diaspora in Poland with their compatriots involved in armed jihad in the Syrian conflict zone and in their country of origin are conducive to radicalisation. Young members of this diaspora look up to fighters in Syria as role models, both in terms of their religious attitudes and combat skills. Therefore, combat sports clubs attended by representatives of this diaspora are becoming centres of radicalisation. The former role models of fighters struggling for the country's freedom are increasingly often replaced by jihadist fighters. This diaspora in Poland is one of

[213]https://przemysl.naszemiasto.pl/wsrod-ponad-miliona-uchodzcow-byly-33-osoby-poszukiwane/ar/c1-8735507 access on 18.06.2022

the communities monitored by the Internal Security Agency for threats of religious radicalisation.

441. On 9 May 2019, Internal Security Agency officers detained[214] in Warsaw a Polish citizen, Mikołaj B., suspected of preparing to commit a terrorist offence in Poland. The detainee was a member of the Muslim community in Warsaw. Unofficially, he goes by the name Mohammed. According to the ABW materials, Mikołaj B. declared his intention to carry out a terrorist attack in a public place in revenge against opponents of the Islamic religion. The Masovia Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office presented Mikołaj B. with a charge under Article 119(1) of the Penal Code, punishable by imprisonment from 3 months to 5 years. Mikołaj B. pleaded not guilty to this charge. The court applied a preventive measure to the detainee in the form of provisional custody for a period of 3 months. In the past, Mikołaj B. received psychiatric treatment. The investigation into this case was conducted by the Internal Security Agency under the supervision of the Masovia Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Warsaw.

442. Poland is not completely free from threats posed by foreign fighters either. According to the available information, several dozen people directly related to Poland have gone to Syria in recent years, where some of them have taken active military action supporting Islamic terrorist groups. This group included foreigners (mainly Chechen nationals) who went to Syria having a legal residence status in the Republic of Poland, although they lived in other European countries. These people may gradually return to Europe, including Poland. According to the data contained in the TE-SAT 2021 report, approx. 5,000 European FTFs went to the conflict zones in Syria and Iraq. In 2020, the estimate of the total number of EU FTFs remaining in the conflict zone remained unchanged – most likely not only due to the restrictions introduced by the COVID-19 pandemic, but also as a result of reduced support for jihadist groups in Syria and Iraq as well as increased effectiveness of preventive actions taken by law enforcement agencies in EU countries. Due to the aforementioned factors, it was difficult for EU Member States to verify the current status or location of the fighters.

443. Currently, the level of terrorist threat in Europe is largely affected by the widespread access to online propaganda materials of terrorist groups, which significantly increases radicalisation leading to terrorist acts, i.e. home-grown terrorism. This type of materials are also commented on and distributed by Polish Internet users. To counteract this phenomenon, the EU adopted *Regulation on addressing the dissemination of terrorist content online* in 2021.

444. Besides religiously motivated terrorism, potential threats may also be generated by groups professing extreme political ideologies – both right-wing and left-wing. According to the available information, at present, Polish extremist groups do not pose direct threats to the internal security of Poland. Their activity mainly involves organising demonstrations, celebrations of historical anniversaries, concerts, fighting tournaments and other activities related to the promotion of extreme ideologies. Representatives of these circles engage in hooligan or criminal activities, inspired by their ideology, only occasionally. The activities of right-wing and left-wing groups are monitored also for hybrid threats and the possible

[214] https://www.gov.pl/web/sluzby-specjalne/mikolaj-b-planujacy-przeprowadzenie-zamachu-zatrzymany-przez-abw access on 18.06.2022

inspiration of some groups by people related to the secret services of foreign countries (also to organise terrorist acts).

445. However, in 2021, a judgement was passed in Poland regarding preparations for a terrorist attack by a member of an extremist group presenting far-right views. Marcin K., who was investigated by the Internal Security Agency, was sentenced to five and a half years in prison and a fine for preparing a terrorist attack using explosives. Marcin K. was a member of a right-wing extremist group operating in Poland until 10 November 2019. The group modelled its plans on terrorist attacks committed by far-right extremists, among others by Anders Breivik in 2011 in Norway and Brenton Tarrant in 2019 in New Zealand. The accused intended to carry out similar attacks in Poland using explosives, targeting places and people belonging to the Islamic community living in Poland. The investigation regarded activities that threatened the lives or health of many people or could lead to large-scale property damage. During their activities, Internal Security Organisation officers collected information about the activities of the extremist group. A number of chemical substances were disclosed and seized, including explosive and drug precursors. Four firearms and ammunition as well as numerous elements used to produce firearms and tools for their production were also seized. On 19 October 2021, a judgement was passed before the Regional Court in Warsaw, to become final on 30 November 2021. Marcin K. was sentenced to imprisonment for 5 years and 5 months and a fine of PLN 1,500. The conviction covered, among others, preparation for a terrorist attack and the production and possession of firearms and ammunition. The investigation into this case was conducted by the Szczecin Branch of the Gdańsk Regional Office of the Internal Security Agency under the supervision of Szczecin Branch of the National Prosecutor's Office[215].

446. At the end of September 2020, officers of the Internal Security Agency detained a German citizen suspected of participating in an organised criminal group involved in terrorist activities and operating in Poland and other countries. The suspect was detained in the Kujawsko-PomorskieVoivodeship. The ABW findings regarding the detainee indicated that he may have weapons and explosives. The detainee presented online, mainly on social media, radical anti-system views and supported extreme right-wing organisations. When searching his place of work and residence, the officers found explosives (cast and pressed TNT) with a total weight of 1.2 kg[216]. Ammunition for combat and alarm firearms, a fuse, a tear gas grenade and electronic data carriers were also seized.

447. The conditions resulting from the COVID-19 pandemic created new opportunities for extremist groups that decided to spread their ideology outside their traditional circles. According to the Terrorism Situation & Trend Report (Te-Sat 2021), Poland recorded, for example, that extremist groups used new recruitment strategies. These strategies included increasing the popularity of extremist groups among those segments of society that are not typically interested in their ideology. Slovakia reported that extremist groups organised demonstrations and protests against COVID-19 restrictions and lockdowns. COVID-19-related arson attacks on telecommunications towers (related to 5G technology) were also reported. At the beginning of the pandemic, Poland also witnessed numerous cases of vandalism targeting telecommunications infrastructure.

[215] https://www.gov.pl/web/sluzby-specjalne/wyrok-za-przygotowanie-zamachu access on 18.06.2022
[216]https://www.abw.gov.pl/pl/informacje/1693,Obywatel-RFN-zatrzymany-przez-ABW.html access on 26.06.2022

448. The Internal Security Agency fulfils its statutory obligations on an ongoing basis. Its tasks are defined in Article 5 of the *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (Journal of Laws of 2023, item 1136). These include, among others, "identifying, preventing and combating threats to the internal security of the state and its constitutional order, and in particular to its sovereignty and international position, independence and integrity of its territory, as well as the state's defence". As part of its activities, the Internal Security Agency monitors radical circles. Due to the nature of radical organisations' activities, the Internal Security Agency conducts operational and analytical activities in this regard. In accordance with its statutory obligations, the Agency provides the most important figures in Poland with reports and studies on extremist threats in Poland[217].

449. False alerts about the planting of explosive charges, due to their social harmfulness and disorganisation of the operation of the entities to which they relate (including public institutions and public utility facilities), are a potential threat to the lives and health of evacuated people, e.g. in hospitals), while the financial outlays incurred as a result of such alerts are a major problem from the state's perspective. The disinformation nature of false alerts about the planting of explosives may potentially be used by terrorist organisations in the tactics of carrying out actual attacks, and may also be used to test the readiness and methods of operation of the relevant services.

450. As regards identifying and combating terrorist threats and criminal terror, in 2022, the Central Investigation Bureau of the Police recorded nine cases of explosions caused by the use of explosive materials and devices (eight and six such cases were recorded in 2020 and 2021, respectively). The reasons for the aforementioned explosions were as follows: three cases of detonation of an explosive material or an explosive device during its production (no case in 2021); two cases of intentional explosion of an improvised explosive device, planting an explosive device (two cases in 2021); two cases of defusing and tampering with unexploded ordnance of military origin (two cases in 2021); two unfortunate accidents while working with pyrotechnic materials (two cases in 2021). The Central Investigation Bureau of the Police did not record any cases of acts of criminal terrorism in 2021 and 2022.

451. As far as combating organised criminal crime is concerned, in recent years, CBŚP officers have dealt, among others, with combating organised criminal groups engaged in the illegal production and trafficking of weapons and ammunition, theft of luxury cars, and kidnapping for ransom. In 2022, the CBŚP seized a total of 599 pieces of firearms (370 in 2020 and 760 in 2021), including: short-barrelled – 169 pieces, long-barrelled – 332 pieces, submachine guns – 60 pieces, gas guns – 22 pieces, improvised explosive devices – 5 pieces, and other weapons, i.e. signal guns, alarm guns, hand cannons, bullet guns converted from gas guns – 11 pieces[218].

452. The structure of the Internal Security Agency includes an Counter-Terrorist Centre (CAT ABW) that serves as a coordination and analytical unit for counteracting and combating

[217] Response of the minister – coordinator of special services of 28 February 2018 to parliamentary question No. 19011 (on information on extremist threats, provided to the President of the Republic of Poland and the Prime Minister by the secret services), at: http://search.sejm.gov.pl/SejmSearch/ADDL.aspx?DoSearchNewByIndex.
[218] Sprawozdanie z działalności Centralnego Biura Śledczego Policji za 2022 rok (w ujęciu statystycznym) (Report on the activities of the Central Investigation Bureau of the Police for 2022 (statistical approach), Warsaw, 2023, at: http://www.cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

terrorism. The CAT ABW operates 24 hours a day, 7 days a week. Besides ABW officers, its structure includes also officers, soldiers and employees seconded, among others, from the Police, Border Guard, Foreign Intelligence Agency, Military Intelligence Service, Military Counterintelligence Service and the National Revenue Administration to carry out tasks within the competence of the institution they represent. Other entities involved in the anti-terrorist protection system of the Republic of Poland that actively cooperate with the Counter-Terrorist Centre include the Government Centre for Security, Ministry of Foreign Affairs, State Fire Service, GIFI, General Staff of the Polish Armed Forces, Military Police, etc. The core tasks of the CAT ABW include the coordination of the exchange of information between participants of the anti-terrorist protection system to enable 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 that affects 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 funds that may indicate the financing of terrorist activities[219].

453. Due to the cross-border dimension of crime and terrorism, as well as in connection with the abolition of border controls between countries in the Schengen area, international cooperation in preventing and combating threats to internal security has been significantly strengthened. Its main elements include, among others, the international exchange of information between competent authorities that makes it possible to identify people posing a threat. The services subordinated to and supervised by the Minister of the Interior and Administration are continuously developing international cooperation, using available mechanisms, such as the Schengen Information System II (SIS II), the European Union Agency for Law Enforcement Cooperation (EUROPOL) or the Prüm Decisions.

454. From the perspective of the internal security of the state, a particular threat is posed by the links between illegal migration and organised crime and terrorism. Migration processes may be related to terrorism through the use of strike groups or sleeper cells. The strike group strategy assumes infiltration into the territory of a given country in order to carry out a terrorist attack previously planned on the territory of another country. The sleeper cell strategy consists in the use of sleeper cells, i.e. groups already located on the territory of the target country, that are activated at the right moment to carry out a terrorist attack. In this case we are usually dealing with home-grown terrorism. Regardless of these two strategies, terrorist attacks are increasingly often carried out by people acting alone, referred to as lone wolves or lone actors, inspired by generating increasingly radical sentiments.

455. On 16 October 2020, based on a decision of the Minister of the Interior and Administration, a 61-year-old Lebanese citizen was deported to his country of origin[220]. The Lebanese was suspected of supporting the Islamic State. The man was detained on 16 April 2020 by the Border Guard. Based on materials collected by the Internal Security Agency, it was established that the man planned to organise, in the Republic of Poland and other EU countries, a network aimed at organising and carrying out terrorist attacks in Western European countries.

[219] https://www.gov.pl/web/mswia/abw , access on 18.06.2022
[220] https://www.gov.pl/web/sluzby-specjalne/obywatel-libanu-podejrzewany-o-terroryzm--deportowany access on 18.06.2022

The deported man had family ties with terrorists from the Islamic State who died in battles with coalition forces in Syria and Iraq. Throughout his stay in Poland, the Lebanese was in constant contact with the structures of the Islamic State using online means of communication. He communicated with people linked with this organisation residing in EU countries. He also financially supported members of the Islamic State remaining in Syria. A five-year ban on entry into the territory of the Republic of Poland and other Schengen countries has also been imposed on the Lebanese.

456. On 30 January 2019, as a result of cooperation between officers of the Internal Security Agency and the Border Guard Post in Warsaw, Nurmagomed M., a citizen of the Russian Federation of Chechen origin, was detained[221]. The foreigner had links with terrorist organisations and was involved in providing logistic support to such organisations. The detained Chechen was also a member of an organised criminal group dismantled by the Internal Security Agency in 2018, consisting of Russian citizens of Chechen origin, that supported terrorist organisations. He collaborated with Azamat B., deported from Poland in August 2018 at the request of the Head of the Internal Security Agency. By a decision of the Head of the Office for Foreigners, Nurmagomed M. was deprived of the subsidiary protection he had enjoyed in the Republic of Poland since 2009 and was entered into the "List of foreigners whose stay on the territory of the Republic of Poland is undesirable".

457. At the beginning of May 2020, based on materials collected by the Internal Security Agency, the Border Guard detained[222] four citizens of Tajikistan who were recruiting other people for terrorist activities. The ABW materials showed that the detained foreigners were recruiting in Poland people converted to Islam in order to carry out terrorist activities. The collected material showed that the detainees supported the activities of a terrorist organisation, i.e. the Islamic State. The foreigners were detained in a guarded Border Guard facility in order to be deported and included in the list of persons whose stay in the territory of the Republic of Poland and the Schengen area is undesirable. The activities were carried out in accordance with the provisions of the Act on foreigners and the Act on anti-terrorist activities.

458. For years, illegal migration has been the most serious type of border crime, especially in organised forms, whose combating is a priority task of the Border Guard. Illegal migration is constantly growing, with possible changes in the forms and methods of its organising and sources of migration flows depending on geopolitical changes and emerging armed conflicts as well as economic and humanitarian crises around the world. Poland is treated by illegal migrants primarily as a transit country on the migration route to other countries in Western Europe and North America, but for a relatively small number of them it is also a country of destination due to, among others, Poland's favourable geographical location at the crossroads of Europe's main communication routes; Poland's membership in the Schengen area, and thus easy access to Western European countries, better economic and social prospects, an attractive labour market, better earnings as well as social and living conditions, and political, religious and moral freedom. As for migration to Poland, a lot has changed after Russia's aggression

[221]https://www.gov.pl/web/sluzby-specjalne/zatrzymanie-nurmagomeda-m-powiazanego-z-organizacjami-terrorystycznymi access on 18.06.2022
[222] https://www.gov.pl/web/sluzby-specjalne/zatrzymano-werbownikow-panstwa-islamskiego access on 19.06.2022

against Ukraine. Poland's opening to refugees from Ukraine has made Poland the main destination for war refugees, followed by Romania.

459. According to available information, Border Guard officers have carried out a number of operations resulting in the dismantling of organised criminal groups, including international ones, operating in many countries and dealing with illegal cross-border transfer of foreigners. In connection with participation in an organised group or in an association aimed at committing an offence:

- in 2021, the Border Guard initiated 90 preparatory proceedings. A total of 512 suspects were charged with committing an offence, including 110 foreigners, mainly Ukrainians (69). Fifty-seven preparatory proceedings were completed. As regards crossing the border contrary to the regulations (punishable under Article 264(2) of the Penal Code and Article 264(3) of the Penal Code), the Border Guard initiated 1,765 preparatory proceedings in 2021. A total of 3,136 suspects were charged with committing an offence, including 3,016 foreigners, mainly Iraqi citizens (687). The number of completed preparatory proceedings was 1,295.
- in 2022, the Border Guard initiated 74 preparatory proceedings. A total of 445 suspects were charged with committing an offence, including 94 foreigners, mainly Ukrainians (35) and Belarusians (23). Forty-eight preparatory proceedings were completed. As regards crossing the border contrary to the regulations (punishable under Article 264(2) of the Penal Code and Article 264(3) of the Penal Code), the Border Guard initiated 1,530 preparatory proceedings in 2022. A total of 3,050 suspects were charged with committing an offence, including 2,064 foreigners, mainly Ukrainians (439). The number of completed preparatory proceedings was 1,319.

460. Illegal migration takes place mainly with the participation of organised criminal groups that organise transport for the transferred people at all stages of their journey, temporary shelter in transit countries, and also provide counterfeit or forged documents. These organised criminal groups use the proceeds from smuggling people across the border to carry out criminal activities in other areas. These groups are extremely creative and quickly adapt their activities to changing legal and practical conditions. There is no single, typical *modus operandi* in this area. Methods of illegal migration include the use of illegal border crossings, crossing the state border of the Republic of Poland based on forged or counterfeit documents, altering border control stamps in order to confirm the "legality" of periods of stay on the territory of the EU and obtain another visa, using the "look alike" method while using documents (especially Polish) belonging to other people. Quasi-legal methods are also used, including: abusing the permit to enter the territory of the Republic of Poland on the pretext of studying, working, for tourist, business or cultural purposes, by using for this purpose false or misleading documents authorising their holder to obtain the relevant visa; abusing the procedure for granting the refugee status in the Republic of Poland or marriages of convenience of foreigners to Polish citizens.

461. The development of terrorism is facilitated by the relatively new phenomenon of the development of the so-called "parallel societies". This phenomenon mainly concerns migrant communities from outside the European cultural circle. Migrants not only do not integrate with the societies of the receiving countries, but – over time – they build barriers and differences, emphasising their own distinctiveness and no chances of lasting understanding. The thus

created social enclaves become “states within a state”, governed by their own laws. Such communities include not only legal immigrants, but also foreigners without a residence permit, who can easily hide in communities that are not in fact subject to checks on the legality of their stay. There is a close link between terrorist activities and human smuggling. The investigation into the 2004 Madrid attacks revealed that the Al-Qaeda-linked *Ansar al-Islam* group involved in the attack was dealing with human smuggling and forging documents, thus financing terrorist activities and transferring its members to Spain.

462. In some countries neighbouring Poland, changes in the terrorist threat level can be seen. The Global Terrorist Index 2023 report noted that Ukraine had significantly improved its position in the region in terms of terrorist threats. The relevant data, obviously, do not take into account the impact of hostilities in this country and related events. Nevertheless, Ukraine did not record any terrorist attacks in 2021-2022, and since 2018, no one has died in this country due to terrorist attacks. Negative developments were, however, recorded last year in Slovakia. The country recorded its first terrorist attack in ten years in October 2022. A 19-year-old man killed two (and injured one) civilians in front of a bar popular among the LGBTQ+ community in Bratislava. Local media reported that the attacker was the son of a former far-right politician who was deprived of his parliamentary seat because he was finally convicted of promoting extremism. The attacker probably did not know his victims, and before he committed this act, he had published a manifesto on the Internet in which he expressed homophobic and anti-Semitic views. He also announced an attack on the house of Slovak Prime Minister Eduard Heger. According to the media, he had recently undergone thorough radicalisation[223].

463. In June 2021, the Terrorist Prevention Centre of the Internal Security Agency drew attention to the EUROPOL’s European Union Terrorism Situation and Trend report – TE-SAT 2020. The Centre noticed that in this report, state-sponsored terrorism had become a new category of terrorist offences. EUROPOL drew attention to the existence of a new form of terrorism, sponsored and carried out by states through secret services. In this case, acts of terrorist violence are committed also to intimidate and eliminate the diaspora living abroad being in opposition to state governments. The TE-SAT 2021 report described, among others, murders of people of Chechen nationality recorded in France, Austria and Germany and planned attacks on gatherings of the Iranian minority, whose activity was contrary to the interests of their countries of origin. In this context, EUROPOL also pointed out, among others, that in 2020, the German Federal Prosecutor General accused a Russian citizen, Vadim K., of murdering a Georgian citizen of Chechen origin in Berlin in August 2019. It was stated in the indictment that the crime was committed on behalf of government institutions of the Russian Federation. In order to commit the crime, the perpetrator took advantage of the opportunity to move freely and unhindered through the Schengen Area. As EUROPOL points out, for this purpose, he went from Moscow through Paris to Poland, and after leaving the hotel in Warsaw, he went to Berlin where he murdered the Chechen.

464. An act of state terrorism has also taken place in Poland. This was the hijacking of a Ryanair[224] plane on 23 May 2021. As announced by Stanisław Żaryn, the spokesman of the

[223]https://wiadomosci.gazeta.pl/wiadomosci/7,114881,29025917,atak-na-klub-lgbt-w-slowacji-zuzana-czaputova-oddala-hold-ofiarom.html access on 20.04.2023
[224]https://polskieradio24.pl/5/1223/Artykul/2865796,Porwanie-samolotu-Ryanair-akcja-bialoruskich-sluzb-Zaryn-przedstawia-dowody access on 17.06.2022

Minister – Coordinator of Secret Services, the Polish investigation into the Ryanair plane case proved that this incident was an operation of the Belarusian secret services aimed at detaining Raman Pratasiewicz who opposed to the political regime of Alexander Lukashenko. After the forced landing in Minsk, blogger Raman Pratasiewicz and his Russian partner Sofia Sapiega were detained. The Polish services collected evidence that this was an operation of the Belarusian services. The analysis carried out by the Polish services indicates that in order to force the plane to land in Minsk, false information about a bomb threat was conceived, then the plane's crew was terrorised and the passengers on board were deprived of liberty and freedom. This sequence of events indicates that, according to Stanisław Żaryn, the spokesman of the Minister – Coordinator of Secret Services, we are dealing with something that should be interpreted as state terrorism activities carried out by the Belarusian services. According to investigators' findings, on 23 May 2021, around 9 a.m., the president of the Belarusian air control agency and an officer of the Belarusian secret services entered the operations centre. The president of the Belarusian air control left the centre after talking to the controller's superior. Then the superior informed the controllers that there was a bomb on board the Ryanair plane and it was necessary to bring the plane to the airport in Minsk. At that time, the plane was entering Belarusian airspace. From that moment on, the flight was operated by one controller, supervised by the officer of the Belarusian services. The officer was in telephone contact with another man. The controller informed the pilots about the red alert and the explosive device. This information was supposed to come from the secret services. He also informed about an email sent to European airports, warning about a possible explosion over Vilnius. The email was allegedly sent by a member of Hamas. As the Rayanair plane began to head towards Minsk, the officer of the secret services left the operations centre at the Minsk airport. In the course of the investigation, it was found that the email regarding the alleged bomb reached the airport in Minsk half an hour after the controller informed the pilots about it. The email account from which the message was sent was created using the anonymising TOR network. According to the investigators, it was probably done specifically for this operation. The Ryanair plane, which was carrying 132 people, including 6 crew members, landed in Minsk after 10 a.m. Representatives of the Belarusian services escorted the passengers out and searched them for the alleged charge. The passengers were searched on the airport tarmac, and after 7 hours the plane departed for Vilnius without 5 passengers, including Raman Pratasiewicz and Sofia Sapiega, his Russian partner.

According to Lithuanian Prime Minister Ingrida Szimonyte, the interception of the plane was an unprecedented act of terrorism against citizens of the European Union and other countries.

465. Acts of state terrorism have also taken place near Poland's borders. In April 2021, the Czech Senate adopted a resolution[225] in which it concluded that an explosion at the ammunition depot in Vrbětice in 2014 was an act of state terrorism against one Member State and thus also against the entire European Union. He requested the Czech government that only the ambassador be left in the Russian embassy and that the agreement on friendly relations and cooperation be terminated. The case concerned an explosion at an ammunition depot in Vrbětice in 2014. Two people, Czech citizens, died in it. According to Czech foreign intelligence

[225] https://www.tvp.info/53430693/czechy-rosja-senat-w-pradze-dzialania-rosji-to-terroryzm-panstwowy access on 18.06.2022

services, the explosion was due to Russian secret services[226]. According to the report from the Czech investigation into the explosion, the attack was carried out by a group of people who later prepared the Novichok attack carried out in Salisbury, England, on Sergei Skripal, a former Russian spy who had defected to the British side. The target of the attack in Vrbětice was supposed to be a supply of ammunition ordered by Ukraine, that was fighting at that time with pro-Russian separatists in Donbas. The planted explosive charges were probably supposed to explode only after the ammunition was transported to Ukraine, but something went wrong and the explosion occurred in the Czech Republic. In connection with the explosion, the Czech government handed the ambassador of the Russian Federation in Prague a diplomatic note demanding compensation. The document reads that Russia is "responsible under international law for participating in the explosion at the ammunition depot" and is also obliged to "pay full compensation for this act of international lawlessness". However, Russia rejected the Czech demands.

6.2. THREAT OF TERRORISM FINANCING

466. Assessment of threats related to terrorism financing covers all aspects of obtaining, transferring, storing and using funds or other assets (including goods, vehicles, weapons, etc.) for the needs of a terrorist organisation, specific individual terrorists or other terrorist activities. The analysis should go beyond aspects related to generating income and should also include ways of transferring funds intended for terrorist activities. It must also cover all persons and organisations that provide funds for terrorist activities and support terrorist activities in any form. It also covers issues related to foreign terrorist fighters (FTFs). Threats related to terrorism financing and terrorist threats are interlinked, but there are also differences between them. This is reflected, for example, in the fact that the threats related to terrorism financing require prior consideration of terrorist threats, both domestic ones and those existing abroad. If there are terrorist organisations in a given country that also operate in other countries or in the region, it is highly likely that their active presence in these countries in the region significantly increases the likelihood of financing terrorism. Given that financing terrorism is a cross-border activity, countries where the terrorist threat is objectively low may, nevertheless, be exposed to an increased threat of financing terrorism. A low terrorist threat in such cases may only mean that lone actors and terrorist groups do not use domestic funds for terrorist attacks or other terrorist activities. However, entities may still exploit vulnerabilities in the anti-terrorism system to raise, transfer or store funds or other assets for terrorist activities in this country. These funds or other assets can also only be transferred through a given country as an intermediary point.

467. It should also be noted that the factors associated with the risk of financing terrorism differ significantly from those associated with the risk of money laundering. While laundered funds come from the proceeds of illegal activities, funds used to finance terrorism may come from both legitimate and illegitimate sources. In the case of money laundering, it is often the case that the conversion of laundered funds may be an end in itself, ultimately leading to the transfer of these funds to a legitimate enterprise, while financing terrorism aims to support acts of terrorism as well as terrorist individuals and organisations, and for that reason the funds or

[226]https://www.euractiv.pl/section/polityka-zagraniczna-ue/news/czechy-chca-od-rosji-odszkodowania-za-wybuch-we-vrbeticach/ access on 18.06.2022

other assets must, for the most part, be ultimately transferred to persons connected with terrorism. Another important distinction is that in the case of money laundering, a money laundering threat is identified based on the operational activities of law enforcement agencies or financial intelligence bodies, while a threat related to terrorism financing, due to the nature of this threat, will need to be more intelligence-led.

468. It is also noticeable that there may be some overlap in the potential vulnerabilities misused by money launderers and individuals financing terrorism. Nevertheless, the motives, and therefore the threat and risk indicators, differ. For example, the transfer of low-volume funds may pose a lower money laundering risk. While transfer of a low volume of funds may entail a lower risk for money laundering, this type of activity (the use of the same product) may pose a higher risk indicator for financing terrorism when considered along with other factors. For example, terrorist financiers use low-limit prepaid cards for purposes related to terrorism financing. Meanwhile, the same instruments (low-limit prepaid cards) used in money laundering are considered to pose a lower risk of money laundering.

469. The financing of terrorism in the Polish legal system has been penalised by amending the provisions of the *Penal Code*, to which the provision of Article 165a has been added on the following grounds: "The requirement to penalise the 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). Financing of terrorism is also addressed in *Directive 2005/60/WE*. In this respect, the above regulation is intended not only to fully implement this Directive, but also to harmonise the application of international standards"[227].

470. As Professor Alicja Grześkowiak[228] states in her commentary to the *Penal Code*, the offence specified in Article 165a of the *Penal Code* should be regarded as an offence in the foreground of an actual terrorist offence, constituting a stage of the preparation for this type of act. The criminalisation of such conduct is intended to ensure counteracting terrorism at the earliest possible stage. The good protected by the provision concerned is public security, and the offence itself is a common one. According to Professor Alicja Grześkowiak, the legislator provided for three different types of offences under Article 165a of the *Penal Code.* Criminal conduct criminalised under the provision of Article 165a(1) of the *Penal Code* consists in raising, transferring or offering legal tenders, financial instruments, securities, property rights or other movable or immovable property to finance a terrorist offence or an offence referred to in Articles 120-121, Article 136, Articles 166-167, Article 171, Article 252, Article 255a or Article 259a of the *Penal Code*. Therefore, it applies to activities relating to measures which would create the conditions for undertaking an act leading directly to any of the aforementioned offences. The legislator has included in a causative act the widest possible range of conduct so that the provision of Article 165a of the *Penal Code* covers conduct that could be considered a manifestation of the financing of terrorism or another of the indicated offences.

471. Conduct consisting in making legal tenders, financial instruments, securities, foreign exchange values, property rights or other movable or immovable property available to an

[227] http://orka.sejm.gov.pl/Druki6ka.nsf/0/387E14C98A33D8BFC125755A004AE7DC/$file/1660.pdf, access on 19.06.2022

[228] *Kodeks karny*. Komentarz, ed. prof. dr hab. Alicja Grześkowiak, prof. dr hab. Krzysztof Wiak, publishing house: C.H.Beck, issue VI, 2018

organised group or association aimed to commit a terrorist offence or an offence specified in Article 165a(1) of the *Penal Code*, to a person participating in such a group or association or to a person who intends to commit such an offence, has also been criminalised. Article 165a of the *Penal Code* also provides for the criminalisation of conduct consisting in covering costs related to meeting the needs or discharging the liabilities of a group, association or person referred to in paragraph 2 of this article. The scope of this provision excludes persons who are obliged to cover the aforementioned costs or liabilities – whereby this obligation results in their case from the Act (e.g. maintenance obligations). In this case, the causative act consists in "(...)providing funds for the livelihood of persons, groups or associations that finance committing terrorist offences. Penalised activities include meeting the everyday needs and discharging financial liabilities of groups that support terrorist activities. The purpose of penalising such acts is to deprive persons supporting terrorism of funds. This is a clear indication addressed to society that providing a livelihood for those who support terrorism is unlawful"[229].

472. Terrorist organisations differ considerably in terms of their size and the nature of their activities. There are organisationally complex terrorist structures that operate like corporations, as well as small, decentralised, and often autonomous networks. Besides organisations, there are also lone actors. Financing requirements of each of the above categories also differ. After all, financing terrorist activities does not only mean covering the costs of carrying out specific terrorist operations, but also ensuring the financing of organisational costs, i.e. the development and maintenance of terrorist organisations and the creation of a favourable conditions necessary to support their activities. The cost of carrying out an attack itself is currently relatively low, given the scale of the damage caused by it or the cost of the resources used for neutralisation or reconstruction. It is expensive, however, to create and maintain a terrorist network (or even a single unit of a terrorist organisation) as well as organise the recruitment of members. Administrative costs of planning, purchasing, communication and infrastructure are also high. Substantial financial resources are needed for terrorist organisations to reach out with the terrorist ideology to their future members, train their current members, broadcast propaganda among the public, and develop certain views and social behaviour. If it is possible to cut off terrorist organisations from the flow of funds, a new situation is created where the hostile ideological influence of terrorist organisations on society and individuals is prevented, and the practical possibilities for such organisations to carry out attacks are significantly reduced.

473. The *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* is the key legal act relating to counteracting the financing of terrorism. This Act specifies the authorities and entities operating in the Polish system for counteracting financing terrorism and specifies their responsibilities and powers.

[229] Rationale for the resolution of the Senate of the Republic of Poland of 16 March 2017 on the Act amending the Act – Penal Code and certain other acts – Form No. 1382, at: http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=1382 (read on 29.05.2019)

474. In 2022, the GIFI[230] initiated 7 (5 in 2021[231]) analytical proceedings regarding transactions that could potentially be related to terrorism financing. The proceedings were conducted based on information received from cooperating units and obligated institutions, as well as information or requests received from foreign financial intelligence units. The proceedings initiated based on information from obligated institutions concerned usually transactions carried out by natural persons from the countries with higher terrorist risk, i.e. ones where terrorist groups are active and from countries where military operations are carried out. The GIFI examined the flows on personal bank accounts and money transfers involving these individuals. In cooperation with the Counter-Terrorist Centre of the Internal Security Agency, the GIFI analysed the links with individuals or entities from countries with higher terrorist risk and identified their links with terrorist organisations. Verification of suspicions of financing terrorism led in some cases to their confirmation or detection of illegal commercial activities unrelated to terrorism financing, or on the contrary – to confirmation that certain transactions were carried out as legal financial activities connected, for example, with family or business ties with entities established in countries with higher terrorist risk. In 2022, the GIFI received 15 (40 in 2021) requests from the Internal Security Agency for information on individuals and entities suspected of financing terrorism. The GIFI replied to all requests, forwarding the information received from obligated institutions to the Internal Security Agency. In some cases, the information provided by the GIFI was supplemented with information received from foreign FIUs. As a result of analyses related to the aforementioned issues, the GIFI sent, pursuant to Article 106 of the *Act of 1 March 2018 on counteracting money laundering and financing terrorism*, a total of 11 (8 in 2021) notifications to the Internal Security Agency. In some cases, the GIFI information was supplemented with information received from foreign FIUs.

475. Poland may be considered an attractive country for building a logistic and financial base by terrorist organisations, among others, due to its favourable location, membership in the Schengen Area, etc. Having this in mind, the Internal Security Agency verifies information regarding the possible transfer of funds to finance terrorism that the Agency receives from partner services and institutions or obtains in the course of its operational work. The thus obtained information mostly concerns transfers made through financial institutions or the Hawala system. Due to the specific characteristics of the phenomenon concerned, it is difficult to confirm the actual involvement of a given person/entity in financing terrorism.

476. Despite the existing differences between terrorist groups and even differences within terrorist organisations, what they all have in common is the need to have financial resources they can use to implement their planned terrorist attacks. The funds held by terrorist organisations make it possible for 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 basic purposes of their activities, including: terrorist operations; propaganda; recruitment of new members; training of organisation members; remuneration or compensation for members; and

[230] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2022 roku (Report of the General Inspector of Financial Information on the implementation of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2022), Warsaw, 2023

[231] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 roku (Report of the General Inspector of Financial Information on the implementation of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2021), Warsaw, 2022

ensuring livelihood for the organisation's members and their families. The very methods of terrorist financing used to generate income for terrorist organisations often have regional characteristics and may include: kidnapping for ransom; extortion; funding through charities; cigarette and tobacco smuggling; sale of used cars; drug trafficking; sale/smuggling of cultural goods; smuggling of natural resources; collection of local taxes, etc.

477. In the context of identifying terrorist networks, terrorist organisations or individual terrorists, the ability to track financial operations is of great importance. *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 Program* (OJ L 195/5, 27.07.2010) has been in force since 2010. Under the Terrorist Finance Tracking Program (TFTP), initiated in 2001, the U.S. Treasury Department seeks to identify, track, and prosecute terrorists and their funders. Pursuant to the above Agreement, to obtain the necessary data from the EU, the U.S. Treasury Department submits a request to the designated SWIFT[232] provider in the United States and sends it any additional documents. The Department shall simultaneously forward copies of these documents to EUROPOL. In accordance with the Agreement, EUROPOL, as a European public authority, assesses whether the data required in a given case is necessary to fight terrorism and its financing. EUROPOL also checks whether each request meets the requirements specified in the Agreement. Once the request has been confirmed to meet the requirements, it is legally binding and the designated supplier is required to submit the required data to the U.S. Treasury Department. The provided data is processed solely for the purposes of preventing, investigating, detecting or prosecuting terrorism or its financing. The provided data is protected against unauthorised access, disclosure as well as any unauthorised forms of processing. The search for the provided data is in each case carried out solely on the basis of collected information or evidence that indicates that the entity whose data is being searched may be associated with terrorism or its financing. The search for the provided data and the reasons for such a search must be documented in each case. The downloaded data may be retained only for the period necessary to achieve the purpose for which it was required. The Agreement also sets out safeguards limiting the further transfer of downloaded data. The U.S. Treasury Department must share information from the TFTP that may be used by the EU to take action against terrorism with the relevant authorities of the EU Member States concerned, and, where appropriate, EUROPOL and Eurojust. Likewise, if any additional information is deemed necessary in the U.S. fight against terrorism, it must be transferred back[233].

478. According to data obtained from the Ministry of Justice[234], in 2019, common courts in Poland did not initiate a single criminal proceeding in relation to an offence under Article 165a of the *Penal Code*, nor did they complete a single criminal proceeding under this article. Therefore, in 2019, no person was convicted in the first instance for an offence under Article 165a of the *Penal Code*, and there were no final convictions for financing terrorism. In 2020, common courts in Poland initiated one criminal proceeding in relation to an offence under

[232] Society for Worldwide Interbank Financial Telecommunication
[233]https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=LEGISSUM:jl0039&from=EN and https://uodo.gov.pl/pl/p/tftp, access on 19.06.2022
[234] According to the information obtained from the Ministry of Justice, the data in this regard is provided by Divisions of Regional Courts (1st instance) and District Courts. What matters is whether the ruling is final or not, it does not matter in which instance it became final

Article 165a of the *Penal Code*, and completed one criminal proceeding under this article. As a result of the proceeding regarding an offence under Article 165 a of the *Penal Code* concluded in 2020, one person was convicted in the first instance, and there were no final convictions in 2020 for financing terrorism. In 2021, common courts in Poland did not initiate a single criminal proceeding in relation to an offence under Article 165a of the *Penal Code*, nor did they complete a single criminal proceeding under this article. In 2022, common courts in Poland did not initiate a single criminal proceeding in relation to an offence under Article 165a of the *Penal Code*, but completed one criminal proceeding under this article. In 2022, no person was convicted in the first instance for an offence under Article 165a of the *Penal Code*, and there were no final convictions for financing terrorism.

479. In June 2020, the Supreme Court overturned the contested judgement convicting three Chechens in a trial regarding, among others, financing terrorism[235], and referred the case for reconsideration to the Court of Appeal in Białystok. In 2017, three Chechens were sentenced to two years and one month in prison. The fourth defendant was acquitted. The defendants were accused of participation in an organised criminal group whose activities in 2014 included, among others, raising funds for terrorist activities carried out by the Islamic State (IS). The charges also concerned organising and purchasing paramilitary equipment and recruiting fighters to take part in jihad in areas of armed conflict. The indictment also mentioned that one of the Chechens who was wounded when fighting in Syria was treated in Poland. The defendants pleaded not guilty throughout the preparatory proceedings and then before the courts of first and second instance. They argued that while the money was raised and transferred, it was not intended for the needs of the IS, but for Chechen fighters fighting for the independence of the Chechen Republic of Ichkeria.

480. In March 2022, the Court of Appeal in Białystok[236], after re-examining the case in question, due to the lack of sufficient evidence, acquitted them of committing the alleged acts (ref. No. II AKa 147/20). According to the judge rapporteur, the case was exceptional, both from the legal and factual point of view. In the course of the trial, studies and analyses regarding the assessment of the geopolitical situation in the North Caucasus, carried out for the court by persons knowledgeable about this region, such as experts from the Centre for Eastern Studies, were unable to draw clear-cut conclusions. They emphasised that the situation in the North Caucasus was exceptionally fluid and dynamic at the time of the defendants' activities, and the political affiliations of the fighters were variable and difficult to be clearly determined, especially as regards the establishment of an organisation considered terrorist, i.e. the Caucasus Emirate, a virtual and non-centralised entity, and then the Islamic State and the interdependencies and connections between fighters presenting different views. At the same time, the experts emphasised that the messages from various sources were ambiguous and often contradictory. The information provided by the parties involved in the conflict, including the official websites of the Russian ministries responsible for military and law enforcement issues, is difficult to verify due to the lack of operational knowledge and disinformation activities. The court ruled out that the aid provided by the defendants was intended for the Islamic State.

[235]https://prawo.gazetaprawna.pl/artykuly/1483707,sad-najwyzszy-wyrok-czeczenia-terroryzm.html, access on: 19.06.2022

[236]https://bialystok.sa.gov.pl/informacje-rzecznika-prasowego/1724-troje-oskarzonych-prawomocnie-uniewinnionych-od-zarzutu-finansowania-terroryzmu.html?tmpl=component&print=1&layout=default&page= access on 14.06.2022

481. The Court of Appeal did not share the assessment of the evidence made by the Court of first instance and the conclusions drawn from this assessment, nor the interpretation of the provisions of substantive law in the aspect of the application of the principles of intertemporal law. Changes in legal regulations over the years in relation to terrorism financing are relevant to the procedural interests of the accused. At the time of committing the offences charged against the defendants, a different legal regulation was in force than at present, raising and transferring funds to finance terrorist offences was penalised, and the persons accused of such acts had to be proven to have acted with direct, specific intent. It was only later that the penalisation of the subjective and objective aspects of these acts was extended. However, in accordance with the principle applicable in Polish criminal procedure, the law that is more favourable to defendants should be applied to the men accused in this case and any doubts should be resolved in their favour. The judgement is final.

6.3. THE MOST COMMON METHODS USED TO FINANCE TERRORISM

482. For the fight against financing terrorism to be effective, it is necessary to know, detect and counteract all methods of raising and moving funds and other assets by terrorist organisations and their supporters as well as prevent these illegal practices. Action should be taken in such a way that law enforcement agencies can use financial operations to locate terrorists and prevent them from committing offences as far as possible. Counteracting financing terrorism also involves neutralising the sources of income of terrorist organisations by disrupting their ability to raise funds. For state authorities'actions aimed at counteracting financing terrorism to be effective, they must be targeted not only at terrorists and terrorist organisations, but also at their supporters. These actions should cover, among others, foreign terrorist fighters, financial supporters and entities raising funds, as well as any other persons who knowingly support terrorist activities. From the point of view of countries combating financing terrorism, the key instruments used to detect the flow of funds through financial transactions or identify terrorist networks and their supporters include financial intelligence units and tracking systems, such as the TFTP[237].

483. Financing of terrorist activities may be carried out with funds obtained from legal sources (e.g. using charitable organisations or legal business activities), through self-financing and using criminal activities as a method of raising funds. However, financing large terrorist organisations is different from financing terrorist attacks carried out by lone actors or small terrorist groups. Attacks carried out by lone actors or small terrorist groups usually involve unsophisticated methods of operation, such as a knife attack or using a vehicle as a weapon. Such methods of operation usually do not require significant financial resources and can therefore be self-financed by the perpetrators. Financial needs are much greater where perpetrators intend to use firearms, explosives or other more sophisticated methods of attack.

484. *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*, hereafter referred to as Directive 2018/843, explicitly indicates that, based on

[237] 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 at: https://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0009.02/DOC_1&format=PDF.

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 terrorist groups pose a growing threat to EU security. The operating terrorist groups turned to alternative sources of funding, including criminal activities, long ago. The use of criminal activities to raise funds for terrorist purposes ranges from petty offences, such as fraud, to involvement in serious and organised crime, such as arms trafficking, kidnapping for ransom, extortion and drug trafficking.

485. One of the most recognisable financing instruments[238] used by terrorist groups is the sharing of wealth by more affluent members of the Muslim community with the needy, called zakat. […] Zakat […] is an obligatory almsgiving for every follower of Islam who has wealth, unlike sadaqah, which is voluntary. Zakat is also the most recognisable Islamic instrument (of the Islamic community) supporting terrorist activities. However, the transfer of zakat funds should be made for the purpose strictly specified in the Quran[239]. Moreover, zakat in Islam is associated with the concept of purification. Therefore, it is also a specific form of expressing gratitude to God for the wealth that he has allowed people to accumulate. The over-interpretation or conscious misinterpretation of zakat, being is the third pillar of the Muslim faith, has resulted in associating this obligation with the financing of terrorist activities and using this pillar of faith to transfer funds to "Muslim (terrorist) fighters", especially where this obligation is performed anonymously. Zakat is collected either by relevant state authorities (in the case of Muslim countries) or by agencies specially established for this purpose (created primarily among Muslim communities living outside Muslim countries). Zakat fulfils many important purposes of Islamic law – Sharia, bringing numerous benefits, evident to anyone who contemplate the contents of the Quran and the tradition – Sunna, ordering it to be paid. Zakat is essential for the Muslim community because it leads to its improvement, both financially and spiritually, and helps eliminate poverty. Only the abuse of zakat contrary to religious standards leads to purposes related to supporting terrorism.

486. The importance of zakat for financing terrorist organisations has been shown by French researcher Michael Nesterenko. According to him, Al-Qaeda's annual income[240] consisted of: USD 1 billion from trafficking in heroin, USD 1 billion from zakat, and approx. USD 300 million from economic and commercial activities.

487. With the decline in sponsorship of terrorist groups by the so-called sponsoring states, drug smuggling and trafficking in psychoactive substances have become an attractive source of funds for terrorist groups. Highly profitable drug smuggling and trafficking make it possible to raise large sums of money in a relatively short time. The intermingling of people involved in both crime and terrorism in terrorist organisations increasingly blurs the distinction between organisations dealing only in drug trafficking or terrorism. Criminal organisations and terrorist groups develop international networks of influence. Globalisation and the opening of borders have enabled both terrorist and criminal organisations to develop and expand their activities.

[238] Wojskowy Przegląd Prawniczy; kwiecień–czerwiec. Warsaw, 2021; dr Maciej Kędzierski – Reguły ostrożnościowe nieumyślnego przestępstwa finansowania terroryzmu (próba oceny); Based on: K. Sadowa, Zakat – podatek czy jałmużna. Doktrynalne podstawy zakat i współczesne funkcjonowanie instytucji – zarys tematyki.
[239] Ibidem
[240] PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO 6/12; Piotr Pomianowski, Ewa Maćkowiak – Zwalczanie finansowania terroryzmu w świetle prawa obowiązującego w Polsce i we Francji; p. 71.

Law enforcement agencies' investigations and intelligence have identified direct links between various terrorist and drug trafficking organisations. The Global Terrorism Index 2023 report explicitly notes that many criminal organisations increasingly represent themselves as Islamic insurgents. In the statistics, their activities are partly attributed to unknown jihadists.

488. Credit card fraud is another method of financing terrorism mentioned in FATF reports[241]. This mainly concerns offences related to making purchases – via the Internet or telephone – using fraudulently obtained details of another person's credit card. Credit card details are 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 and surname, address, telephone number, card start and end dates, card security number, etc.

489. Tobacco-related crime is also one of the methods of illegal fundraising by terrorist organisations. In 2022, the Central Investigation Bureau of the Police seized in Poland, according to its data, almost 245 million cigarettes and almost 213 tonnes of cut tobacco, while 2021, compared to the last few years, was a record year in terms of the quantities of illegally manufactured cigarettes and tobacco seized. In 2021, the CBŚP contributed to the seizure of a total of 280 million cigarettes and 541 tonnes of dried and cut tobacco. According to the National Revenue Administration data, almost 70 million tobacco products were disclosed in freight traffic in 2021 (data received from the Revenue Administration Regional Offices located on the external border of the EU). It is unknown whether the proceeds of the crime in question were transferred to terrorist funds in Poland.

490. The FATF Terrorist Financing Disruption Strategies 2018 report mentions smuggling and sale of cultural goods as a method of financing terrorism used to generate revenue for terrorist organisations[242]. This is especially important in the case of ISIS and cultural goods taken out of Iraq and Syria. Currently, it is difficult to estimate the annual income of the ISIS on this account. According to the FATF Global Network information for 2022, the operational budget of the ISIS is currently only several dozen million dollars (intelligence data indicates funds in the range of USD 25-50 million), which shows that the ISIS's revenue, among others from smuggling and selling cultural goods, has decreased significantly.

491. *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) COM(2016) 50 final) identifies offences related to wildlife trafficking as a current source of financing of terrorism and related activities. According to the data contained in the EU Action Plan against Wildlife Trafficking[243], wildlife trafficking has now become one of the most profitable types of organised crime in the world. The exact scale of this illegal practice is unknown, but various sources estimate the global proceeds from this crime at EUR 8 - 20 billion

[241] For example, FATF-GAFI Report – Terrorist Financing, FATF, February 2008, pp. 17-18, at: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.
[242] Terrorist Financing Disruption Strategies 2018, FATF, October 2018, p. 11.
[243] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU Action Plan against Wildlife Trafficking: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0087

per annum. It covers a wide range of protected species, including elephants and rhinos, corals, pangolins, tigers and great apes.

492. Another way to raise funds mentioned in the literature is extortion. This crime is committed by people who are members of expatriate communities and at the same time relate to the targets of terrorist activities in the diaspora. The terrorist organisation taxes the diaspora's income and savings and enforces the imposed tax. Extortion is generally targeted against one's own community that fears retaliation that can be faced if anyone informs the authorities. Terrorist organisations can also threaten to harm relatives who stay in the victim's country of origin, which even more deters victims from reporting illegal activities to law enforcement authorities. Extortion targeted at community members in the diaspora can be a substantial permanent source of funding for terrorist activities.

493. Substantial funds for terrorist activities are also raised through taxes or other charges. This was particularly important in the case of ISIS, where taxes included, among others, withdrawals from bank accounts and the use of vehicles delivering goods. ISIS currently receives proceeds from leasing agricultural land and taxes collected on crops grown in occupied territories; taxes levied on livestock trade; taxes collected from traders. Dissenters were additionally taxed with *jizya*, a fee/tax for exemption from military service and for defence by Muslims, as well as the privilege of living in Muslim territory. Currently, attempts to introduce *jizya* have been reported in Egypt. Numerous cases of *jizya* extortion have also been 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 – a separatist terrorist organisation of the Spanish Basques.

494. Kidnapping is yet another form of raising funds for terrorist activities. In 2008, a Polish engineer-geologist staying in Pakistan as an employee of Geofizyka Kraków, a company owned by PGNiG, was kidnapped. The kidnappers demanded the release of over 100 Taliban and the withdrawal of military forces from the Pakistan-Afghan border. Later, they moderated their demands and insisted on paying them a ransom for releasing the Polish citizen. Unfortunately, the negotiations with the terrorists did not bring the intended result and the Pole was murdered. What is the most difficult to address and the most dangerous for the victim is kidnapping[244] committed by Islamic terrorists. However, even in this case, the percentage of citizens of Western countries who have been released is 63 percent, and in the case of abductions perpetrated by other non-state actors – as much as 80 percent. Incidents involving terrorists are a small part of all abductions. The jihadists' *modus operandi* is characterised by the fact that they hold hostages for a longer period of time than is the case with other groups. Most kidnapped citizens of Western countries spend about 3-6 months in captivity, and only 9 percent of them are held hostage for more than a year. Executions of hostages occur in approx. 5 percent of all cases. However, jihadists are the group most willing to resort to this type of solutions and do so on average in 15 percent of all abductions. This applies in particular to kidnapped Americans. Most executions (73 percent) take place within the first 30 days of kidnapping. This

[244] https://bezpieczenstwoistrategia.com/porwania-obywateli-rp-za-granica-cz-1-jak-duze-jest-zagrozenie-i-kto-ma-najwieksze-szanse-na-przezycie/ access on 24.06.2022

shows that money is the most common motive for terrorists' actions. Kidnapping Poles[245] abroad is a marginal phenomenon and occurs much less frequently than in the case of citizens of Western countries[246].

495. Terrorist organisations receive substantial support and funds for financing terrorist activities from and through legal entities, including revenue from business activities of economic operators, from donations (tribute) from ethnic groups from which their members come, from remuneration for the work of members or supporters of these groups, from selling or letting real estate, from loans and material aid from family, from charity fundraisers or government subsidies, as well as from savings of their members or supporters or benefits received by them.

496. Charitable organisations play an important role in this case. These organisations benefit from public trust, have access to significant and diversified sources of financing, and their financial activities often involve significant cash flows. Some of the charity organisations are known in many countries and operate practically all over the world, often in conflict areas. This provides a framework for carrying out domestic and international financial operations and transactions, often in or near areas most vulnerable to terrorist activities. At the same time, charities – as non-profit organisations – are subject to much more lenient regulatory requirements than financial institutions or commercial companies (this applies to capital requirements, certificates of professional qualifications, ongoing accounting, reporting and monitoring). The methods used to raise and transfer funds intended for terrorist activities using charitable organisations include:

(1) diversion of funds through fraud. In this case, the charity operates and performs its tasks in accordance with its statutory objectives. However, some of the funds raised by the charity are used contrary to their intended purpose and are transferred for terrorist activities. In this case, the charity may act as a shell organization for raising funds for terrorist purposes, and at the same time perform the important social functions for which it was established. Funds are usually misappropriated by a few individuals within the charity who have privileged access to them;

(2) using a completely fictitious or fraudulent organisation claiming to be a legitimate charity as a shell organisation for terrorist groups. In this case, funds raised from all sources by the charity are transferred for terrorist purposes, and donors – who have contributed their funds for charitable purposes – are not aware that their funds are used for financing terrorism;

[245] On 27 April 2022, African jihadists in Burkina Faso abducted a Polish citizen. The man spent nearly two months in captivity of Islamists. Polish consular services and his family were involved in efforts to release him. On 24 June 2022, the Pole was released by the Ministry of Defence of Burkina Faso. However, no details regarding the release were provided. There is also no information about the conditions for the release of the abducted Polish citizen – https://www.pap.pl/aktualnosci/news%2C1271829%2Cporwany-w-kwietniu-w-burkinie-faso-polak-zostal-uwolniony-jest access on 16.08.2022

[246] In October 2014, a Polish missionary, pr. Mateusz Dziedzic, was kidnapped in the Central African Republic. The Democratic Front of the Central Africa People (FDPC) was responsible for the kidnapping. The kidnapping was supposed to force the release of the rebels' boss, Abdoulaye Miskine. By decision of the Minister of Foreign Affairs, an inter-ministerial team was established whose task was to coordinate activities related to contacts with partners participating in negotiations regarding the release of the priest. Mateusz Dziedzic was released in November 2014.

(3) the so-called broad use – this is the case where a charitable organisation operates in accordance with its statutory tasks, performing socially useful activities for the good of society, but does it through a known terrorist organisation. The charity's operation is therefore also aimed at supporting a terrorist organisation.

497. The National Prosecutor's Office, that supervises investigations in terrorist cases, has not yet conducted analyses of the involvement of non-governmental organisations, in particular foundations and associations, in financing terrorism. However, it is noteworthy that in the investigation regarding four citizens of the Russian Federation accused of financing terrorism, carried out by the Podlasie Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Białystok, it was found that employees of one of the foundations providing humanitarian aid to refugees from Chechnya were used to provide material support in the form of paramilitary products to individuals conducting terrorist activities. However, the foundation itself was not involved in financing terrorism.

498. The activities of terrorist organisations (both those strictly related to terrorist activities as well as logistic and recruitment ones) may also be financed with funds from legal business activities. Income from legal activities comes primarily from those sectors of the economy where no formal qualification requirements (such as a master's certificates, licences) have to be met to start a business and where starting a business does not require significant investment. The risk that a company will divert funds to support terrorism is greater where the relationship between reported sales and actual sales is difficult to verify and in the case of capital-intensive activities. The international network of companies belonging to Osama bin Laden is the example of the link between legal economic activity and using its revenue for terrorist purposes that is most often referred to in the literature[247]. The said network included, among others, a construction corporation, transport companies, an ostrich farm, a bank, shrimp fishing vessels, oil factories, a confectionery factory, diamond mines and many other entities.

499. Terrorist activities may also be financed from internal sources, including funds provided by the family, income from one's own work and other non-criminal sources. The amounts of money needed to carry out small attacks can be raised by individual terrorists and their support networks using savings, access to loans, or other profits from activities they control. Terrorist organisations may be largely decentralised, and self-financing may also include cases where funds are provided by an autonomous external entity that is not directly involved in the planning or execution of the attack, despite providing funds for this purpose.

500. As for the sources and methods of financing ISIL, Al-Qaeda and their associated terrorist organisations, information provided by the FATF Global Network in 2022 shows that the most popular forms of financing these organisations include: raising money through extortion from enterprises in the region of operation of these terrorist organisations; kidnapping for ransom; fees at established checkpoints in those regions of Syria and Iraq where there is a security vacuum or that are controlled by ISIL; revenue from books and publications supporting radical views; revenue generated from hydroelectric power plants in the regions under their control; revenue from the sale of material goods left behind by people leaving the areas occupied by ISIL; revenue obtained from the dismantling and sale of factories in the controlled territories; revenue from the lease of agricultural land and taxes collected on crops in occupied

[247] For example, Brunon Hołyst, Terroryzm. Tom 1, publishing house: LexisNexis, Warsaw, 2009

territories; cryptocurrency donations via Over the Top (OTT) applications; taxes levied on livestock trade; revenue obtained from the appropriation of gold and money from banks located in ISIL-occupied territories; taxes collected from traders; proceeds from looting and smuggling of monuments in occupied areas; revenue from the sale and smuggling of weapons and ammunition seized in conflict zones; revenue obtained from agricultural products, livestock and the sale of stolen goods, revenue from illegal oil trade; funds sent by the families of foreign terrorist fighters (FTFs) who are still active or missing in action; donations to charity that are actually sent to ISIL; consumer loans taken out by ISIL supporters; abuse of social support (benefits, allowances) part of which is sent to ISIL; fraud.

501. According to the available information, while conducting its operational and analytical activities, the Internal Security Agency recorded the following methods of raising funds in Poland to support terrorist organisations:

- income from work (legal and illegal),
- financial support from family members,
- financial support from diaspora members,
- fundraisers conducted under the guise of charity support (including online),
- fundraisers conducted on behalf of a terrorist organisation (voluntary and forced),
- proceeds from criminal activities (smuggling, fraud, extortion, drugs, etc.).

502. Cases of financing terrorist organisations through the transfer of valuable electronic items (e.g. video cameras), sent by post or carried in luggage by travellers, have also been reported.

503. The Internal Security Agency has also recorded cases where funds obtained by members and supporters of terrorist groups were invested in Poland, among others in businesses related to them (or to establish new ones), whose income was then allocated to a given organisation, as well as to purchase real estate by these persons (in some cases such purchases were not commercially viable, e.g. concerned real estate in poor technical condition).

504. As for the movement of funds obtained for terrorist purposes, the FATF report of 29 February 2008[248] on the financing of terrorism lists three main methods of movement of money and values by terrorists. The first method consists in the use of the financial system, the second requires the physical movement of money (for example, by using cash couriers), and the third one involves the international trade system. On the other hand, the FATF Terrorist Financing Disruption Strategies 2018 report lists the following main mechanisms used by terrorist groups to transfer funds: the banking sector; crowdfunding; MVTS, including Hawala; prepaid cards; trade in high-value goods; virtual currencies and other digital carriers of value; and physical transportation of cash[249].

505. As contemporary terrorism consists of organisationally diverse structures, there is a constant evolution of techniques used in response to international efforts to counteract this phenomenon. Although it is difficult to determine which technique is the most common method

[248] For example, FATF-GAFI Report - Terrorist Financing, FATF, February 2008, at: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.
[249] Terrorist Financing Disruption Strategies 2018, FATF, October 2018, p. 11.

of transferring money for terrorist purposes, it seems that – from the point of view of the activities of terrorist organisations – the use of the banking system is the most convenient. In this way, activities closely related to terrorist activities, such as logistics or recruitment, can be easily financed. Money can be transferred using the banking system both within one country and it can also be transferred from one country to another. Fund transfer transactions may be disguised by using accounts kept in false names, for charities or companies to conceal the ultimate payee. Using a bank account to transfer funds may involve transferring both legal and illicit funds to countries embroiled in conflicts or those bordering countries where terrorist organisations operate. Funds are often transferred to accounts in financial and credit institutions located in jurisdictions that do not comply with international AML/CFT standards and recommendations. Bank accounts held by natural persons associated with terrorists (family and other close contacts) can be used to make cash deposits and then cross-border transfers. Terrorists (especially lone wolves) often finance their activities also with their own funds deposited in bank accounts (often from completely legal sources – earnings, loans, scholarships, donations from family).

506. According to one of the definitions of crowdfunding, it is a type of raising and allocating capital transferred for the implementation of a specific undertaking in exchange for a specific return benefit, which involves a wide range of capital donors and is characterised by the use of ICT technologies as well as a lower entry barrier and better transaction conditions than market ones. In the case of raising and sending funds for terrorist activities, we are dealing primarily with donation crowdfunding. The official fundraising purpose will not directly indicate the intention to use the raised funds to finance terrorism. The fundraiser's organisers (supporters of a terrorist organisation) send requests for funds using applications, e.g. Twitter. Once they have found people willing to participate, they also contact them via instant messengers, e.g. Skype. Donors make cash donations to the initiators of the campaign or buy international prepaid telephone cards whose numbers are then made available to them.

507. Alternative money order systems operated in the EU by payment service providers under applicable regulations are also used to move funds for terrorism-related purposes. The use of alternative remittance systems is driven by poorer or less clear accounting and less stringent regulatory oversight. The level of anonymity in relation to banking products is also higher.

508. The informal financial system called Hawala or hundi is another type of alternative financial transfer system used by terrorist organisations due to its anonymity, convenience, speed and accessibility. The term Hawala itself comes from the Arabic language and means a transfer or remittance, originally used by merchants in South Asian countries to safely transfer money. The Hawala system is based on the principle of compensation and relies solely on trust between system participants. Fund transfers using Hawala were made, among others, in the preparation for the attacks on the World Trade Center and the Pentagon in 2001. Nowadays, the Hawala system is based on a network of agents called *hawaladars* or Hawala banks, usually operating unofficially, under the guise of another business activity, e.g. a travel agency, currency exchange office, laundry, restaurants, kebab bar, forwarding company, etc. Hawala agent are particularly active in Pakistan, India and the United Arab Emirates. A Hawala agent runs in fact an underground bank, lending funds, accepting deposits and making transfers around the globe, with virtually no use of the official banking system, using one-time passwords

(tokens) such as quotes from the Quran, names, pre-arranged words or a code of numbers that the depositor in one country shares with the agent and the person receiving the money in another country provides when receiving the thus transferred amount. The most important features of the Hawala system include the speed of transfers, anonymity, the ability to transfer virtually any amount, the lack of any formalities or documents, and being completely invisible to the official banking system. Cost-effectiveness, reliability and tax avoidance are also important. The 2013 FATF report points to the existence of various types of Hawala agents, ranging from those operating officially, as far as possible, through a hybrid model, often remaining invisible to the relevant services, and the typical criminal and illegal model of agents. Hawala transactions are made immediately after the agent has received cash and has been provided with the token. When accepting cash from the sender, the agent immediately orders, via fax, email, telephone call, chat, entry on a social networking site, advertisement on the Internet, or in another unsuspicious manner, the payment of funds in another country. The received money is not transferred through the banking system, and the funds are compensated on a "two-pot" basis. According to this principle the agent will then make withdrawals from the amount received from the sender, because the money does not have to be immediately physically transferred to another agent. The debt will be settled when the agents have balanced deposits and withdrawals. The whole procedure is based on trust between the agents, and any differences are compensated every few years. Compensation can be made through couriers. Hawala couriers usually do not transport cash, but gold, diamonds and valuable antiques that can be cashed in by agents immediately after transportation. The informal banking system makes it possible to maintain complete anonymity of both the sender and the recipient, using several agents when ordering a transfer. In this way, Hawala system operators usually do not know from whom, for what, and to whom the transaction is made, thus they are not necessarily involved in the international terrorism system. What matters most is trust between agents. Informal banking leaves no visible traces indicating that a transaction has been made. Moreover, the cost of making a transaction is much lower than in a traditional bank. Money transferred through the Hawala system 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 UK, where there are many agents offering underground banking services. This is due to the large concentrations of immigrants from the Middle East, India, Pakistan and the Philippines in these countries[250].

509. As countries and international organisations take increasingly new measures to counter the financing of terrorism, especially with a view to applying customer due diligence 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 via couriers is one from the ways in which terrorist organisations move their funds. In this way, they bypass the safeguards established based on the International Standards for Counteracting Money Laundering and Financing of Terrorism in place in financial institutions. Terrorist organisations using couriers to transfer funds for terrorist purposes often exchange money for other values, e.g. gold bars (or jewellery, precious stones, etc.) to move assets outside the financial system. Terrorists may store their assets, for example in gold, because its economic value is easy to determine and remains relatively constant over time. Moreover, given the cultural importance of gold in many

[250] http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu/, access on 22.06.2022

areas of the world, such as Southeast, South and Central Asia, the Arabian Peninsula and North Africa, there will always be demand for gold. Counter-terrorism operations 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, more complex funds transportation plans involve indirect air routes using multiple cash couriers and currency conversions. The movement of money for terrorist purposes via couriers across borders is predominant in countries where electronic banking systems are underdeveloped or are little used by the population. In much of Africa and the Middle East, societies rely heavily on cash, which increases the use of couriers or alternative money transfer systems. Analysis of a number of terrorism cases has shown that money couriers are also active in Europe, even in countries with a sound financial system. In most cases, couriers are involved in moving funds generated outside the financial system and held outside it in order to avoid their detection. Moving funds using money couriers can be relatively expensive compared to bank transfers. However, as legitimate financial institutions tighten their procedures and apply due diligence, using couriers has become an attractive method of transferring funds without leaving a transaction trail. The transported amounts of cash, transferred by terrorist organisations for purposes related to terrorist activities, may be very low, which makes it difficult to detect them and enforce prohibitions/restrictions on transporting them across borders. Moreover, couriers do not leave an audit trail for law enforcement agencies.

510. Funds for terrorism-related purposes may also be moved using virtual currencies. In Poland, the *Act of 1 March 2018 on counteracting money laundering and financing terrorism* defines virtual currency as a digital representation of value that is not:

- a legal tender issued by the National Bank of Poland, foreign central banks or other public administration bodies,
- an international unit of account established by an international organisation and accepted by particular 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 cheque

and is convertible in commercial transactions into legal tenders and accepted as a means of exchange, and may be electronically stored or transferred or may be traded electronically.

511. In a more common sense, virtual currencies include cryptocurrencies and some other conventional units that can be exchanged for regular money, e.g. currencies in some computer games. Virtual currencies can be used to transfer assets for terrorist purposes due to their features that facilitate the anonymisation of the parties to the transaction and make it difficult to track and stop transfers. However, the 2020 TE-SAT report notes that the number of cases related to the use of cryptocurrencies for financing terrorism in 2020 was low. Nevertheless, it should be noted that the potential of using cryptocurrencies to finance terrorism was highlighted in August 2020, when the U.S. Department of Justice announced the dismantling of three

terrorist financing cyber-enabled campaigns, involving the al-Qassam Brigades, Hamas's military wing, al-Qaeda, and Islamic State of Iraq and the Levant (ISIS). The actions of the American services represented the government's largest-ever seizure of cryptocurrency in the terrorism context[251]. These terror finance campaigns carried out by the aforementioned terrorist organisations relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world. The action carried out by the U.S. Department of Justice demonstrates the similarities in raising and transferring funds by various terrorist groups. They adapt their activities related to terrorism financing to the development of technology and new cyber tools. Each of the terrorist organisations used cryptocurrencies and social media to attract attention and raise funds for their terrorist activities. In August 2020, U.S. authorities seized millions of dollars, closed over 300 cryptocurrency accounts, four websites, and four Facebook pages – all related to terrorism financing. In Poland, the number of reports about the possible use of virtual currencies to finance terrorism is small.

512. Prepaid cards are also used to move funds for terrorism-related purposes. The risk of using this product for financing terrorism results mainly from its anonymity and the possibility of crediting accounts linked to it by third parties (e.g. by transfer to a technical account). In Poland, in 2015, as a result of its supervisory activities, the Polish Financial Supervision Authority suggested to issuers (banks) supervised by this institution that it was inadmissible to issue and handle prepaid cards under the existing regulations. This position was based on a very conservative treatment of electronic money and its relation to prepaid cards. According to the Polish Financial Supervision Authority, a prepaid card should not be considered electronic money, which affects banks' obligations as regards issuing and handling prepaid cards. As a result of the activities carried out by the supervisor, there are currently several dozen issuers of prepaid cards on the Polish market that operate under the EU single passport regime, while Polish issuers have adapted to the aforementioned interpretation of the Polish Financial Supervision Authority. However, from the point of view of competition between Polish banks and banks from other EU Member States, it is important that in other Member States prepaid cards with a technical account are recognised as electronic money (including Hungary, Italy and the United Kingdom)[252].

513. At the same time, according to the available information, as a result of its operational and analytical activities, the Internal Security Agency recorded the following methods of transferring the collected funds outside the borders of the Republic of Poland:

- through banking systems,
- using cash transfer agencies,
- through the Hawala system,
- using couriers.

Movable property in the form of electronic products transferred with the intention of financing a terrorist offence was transported via postal items or transported in luggage by travellers, e.g. to Syria.

[251] https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns access on 14.06.2022

[252] Government position of 25 March 2016 on the Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing.

514. One of the basic tasks of the prosecutor's office is to prosecute offences, including those relating to terrorism financing. Five examples of preparatory proceedings relating to such offences are presented below.

Example 1

The Department for Organised Crime and Corruption of the National Prosecutor's Office supervised proceedings regarding the transfer of funds in the territory of the Republic of Poland as well as outside Poland, with the intention of financing a terrorist offence, i.e. an act punishable under Article 165a(1)of the Penal Code, carried out by the Internal Security Agency in 2022.

The proceedings were initiated based on information from Italian law enforcement agencies (sent pursuant to Article 7 of the Convention on Mutual Assistance in Criminal Matters between EU Member States of 29 May 2000) regarding suspected financing of terrorism involving citizens of the Russian Federation residing in the Republic of Poland and Polish citizens being the recipients of the financial transfers. The criminal activities of the aforementioned individuals were disclosed during an investigation conducted by the Milan Prosecutor's Office into the activities of an organised criminal group involved in Islamic terrorism and engaged in forging documents.

In the course of the investigation in this case, explanatory activities are carried out by law enforcement agencies from Austria, Germany, France, Denmark, the Netherlands, EUROPOL and the Prosecutor's Office in Milan. The criminal activities of the suspects also concern Belgium, Finland, Sweden, Norway, Switzerland, Türkiye and Poland. An USB flash drive containing data and photos of several hundred people associated with the Caucasus Emirate terrorist group was seized from the leader of the organised criminal group. It was also found that the several dozen people whose data was saved on this medium are listed in the Schengen/Interpol systems as individuals associated with jihadist terrorism. The investigation is pending.

Example 2

In 2020, an investigation carried out by the Lower Silesia Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Wrocław, ref. No. PK I WZ Ds. 58.2017, was concluded with bringing an indictment.

The investigation covered the circumstances of financing terrorism that occurred in the period from February 2015, at the latest, to April 2016 in Wrocław, consisting in accepting, raising and transferring funds denominated in foreign currencies, i.e. US and Canadian dollars and euro, using the services of Hawala agents.

In the described case, as a result of their operational activities carried out since 2015, officers from the Internal Security Agency detected a group of three individuals of Iraqi nationality (K. R. QB., Ra. K. QB. and Ru. K. QB) who, having settled in Poland, ran a business consisting in making money transfers in the Hawala underground banking system. In parallel with the activities carried out by the Internal Security Agency, the GIFI carried out analytical activities regarding the operations recorded on 15 bank accounts used by the individuals covered by the investigation. The GIFI also analysed Western Union transfers that were sent or received in

branches of Bank BZWBK and PKO BP in Wrocław. As a result of the described analyses three notifications on suspicion of committing an offence were prepared and sent by the GIFI to the prosecutor's office in March and August 2016 and April 2017. The notifications contained detailed information on financial transactions that could be related to terrorism financing, along with bank account records constituting evidence in the investigation.

On 30 August 2017, having received information that the observed individuals intended to leave the territory of the Republic of Poland, the Internal Security Agency detained them and searched the flats occupied by them, as a result of which significant amounts of jewellery and cash, including USD 148,000, were seized.

It was established that K. R. QB., Ra. K. QB. and Ru. K. QB. came to Poland in 2014 and received permanent residence cards. Acting jointly and in concert, they opened a total of 15 bank accounts with Polish banks, namely Bank BZWBK, Millennium and PKO BP. Accounts were opened in three currencies: Polish zloty, US dollar and euro. K. R. QB. also purchased two flats for cash in a prestigious housing estate in Wrocław and founded a company that was used to legalise his stay in Poland.

Then, between March 2015 and September 2017, the individuals concerned received several dozen transfers in the Western Union system from senders located in Iran, Canada, Belgium, the USA, Sweden, Austria and the Federal Republic of Germany. The value of the transfers, identified based on documents secured in the banks, that were received by members of the QB family, amounted to USD 7,800, CAD 4,168, EUR 6,257 and SEK 6,139. At the same time, Ra. QB and three other people not related to the QB family made Western Union transfers in the total amount of USD 627 to M. M. residing in Paraguay.

As established in the course of the investigation, the transfers received by QB family members came, among others, from F. J., M. M., A. N., R. HY and H. S. whose closest relatives were fighters of the Islamic State.

K. R. QB. and Ra. K. QB. were accused of committing offences under Article 165a of the Penal Code read together with Article 12 of the Penal Code in the wording applicable before the amendment that entered into force on 27 April 2017 in connection with Article 4(1) of the Penal Code.

By the judgement of the District Court for Wrocław-Fabryczna, 2nd Criminal Department, of 24 June 2022, the defendants were acquitted of committing the offences they were charged with.

Having considered the prosecutor's appeal, this judgement was revoked in its entirety on 3 April 2023 by the Regional Court in Wrocław, 4th Criminal Department, and the case was referred for re-examination by the court of first instance.

Example 3

The preparatory proceedings were carried out by the Masovia Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Warsaw. The investigation concerned the circumstances of an attempt to set fire to the facade of the building of the Society of Transcarpathian Hungarians – Association of Hungarian Culture in Uzhhorod, Ukraine. The incident took place on 4 February 2018. According to the indictment, the first defendant gave two other persons jackets, SIM cards and mobile phones to record the event, as well as money for this purpose and remuneration for the execution of the order. The

second defendant painted a swastika and the numbers 88, referring to the Nazi greeting "Heil Hitler", on the building's facade and threw a lit bottle of solvent at the building. During the second attempt to set fire to the building on the same day, he placed a jacket soaked in petrol and set it on fire. The third defendant recorded the operation. Ultimately, the facade and one of the windows of the building of the Society of Transcarpathian Hungarians – Association of Hungarian Culture in Uzhgorod, Ukraine, were damaged. Several days later, the Internal Security Agency detained the suspects. They were accused of committing a terrorist offence consisting in painting fascist symbols and setting fire to a building, and one of them was also accused of financing terrorism (Article 165a(1) of the Penal Code). According to the prosecutor's office, the defendants' actions were "intended to publicly incite ethnic hatred between Ukrainians and Hungarians" as well as to "cause a disruption of the political system in Ukraine and deepen national divides between Ukrainians and Hungarians". On 20 March 2020, the defendants were found guilty and the Krakow district court sentenced them in the first instance. The most severe punishment was inflicted on the organiser of the action, namely a three-year prison sentence and a fine of PLN 15,000.

Example 4

The preparatory proceedings were carried out by the Łódź Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Łódź.

The investigation conducted by the prosecutor's office concerned the circumstances of transferring to D. Ł., between October 2018 and 12 February 2019, funds in the amount of USD 1,000 to finance a terrorist offence. The proceedings in question were initiated by a search at D. Ł.'s place of residence, as a result of which the officers seized the said amount of money in USD 100 banknotes as well as computers, telephones and other digital data carriers. These carriers included, among others, instructions for preparing and carrying out terrorist attacks, ISIS propaganda materials and instructions for using firearms. At the place of residence of suspect D. Ł., trace amounts of hexogen were also found. It was established that before he was arrested, D. Ł. stayed in Syria, where he belonged to the Islamic State organisation, and later, during his stay in Norway, he established contact with representatives of the Syrian Islamist group Tahir ash-Sham and the local Islamic organisation Profetens Ummah.

D. Ł. was charged on 28 January 2020 with committing an offence under Article 126c(1) of the Penal Code read together with Article 118(1) of the Penal Code read together with Article 65(1) of the Penal Code. However, the investigation into terrorism financing was suspended pursuant to Article 22(1) of the Code of Criminal Procedure, pending the findings of the Norwegian law enforcement agencies as to the origin of the funds seized at the time of detaining D. Ł.

Example 5

The preparatory proceedings regarding financing terrorism were carried out by the Pomeranian Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Gdańsk. The investigation concerned mainly the participation in 2013-2014 of M. R., having dual Polish and German citizenship, in the terrorist organisation Junud al-Sham and the Islamic State.

Regardless of this offence, during the proceedings, the circumstances of raising and transferring funds and material goods from the Federal Republic of Germany to Syria in order to provide them to members of this organisation were also investigated.

The transfer of money denominated in EUR, as well as electronic products (video cameras) with a total value of EUR 12,547, took place in postal items sent from Germany, personal transport in luggage when traveling to Syria, as well as regular bank transfers or cash transfers in the Western Union system. In the above case, a parallel investigation was carried out in Germany, that ended with an indictment and subsequent conviction of M. R.'s relatives. for financing terrorist activities.

On 21 December 2020, the investigation conducted by the Pomeranian Branch of the Department for Organised Crime and Corruption of the National Prosecutor's Office in Gdańsk was suspended in connection with the search for suspect M. R.

7. VULNERABILITY TO MONEY LAUNDERING AND FINANCING OF TERRORISM

7.1. VULNERABILITY AS REGARDS LEGAL REGULATIONS

515. The operation of the national system for counteracting money laundering and financing of terrorism is based on generally applicable legal regulations, both those that directly relate to this system and those that concern areas only indirectly related to it. These regulations determine the scope of activities, including the obligations and powers of the GIFI, obligated institutions and cooperating units, as well as define the rules for the use of products and services available on the market. The level of their coherence, completeness and adaptation to the existing level of risk of money laundering and financing of terrorism has a significant impact on the effectiveness of the entire system for counteracting money laundering and financing of terrorism.

516. Some of the vulnerabilities were identified and indicated in the 2019 National Risk Assessment. These vulnerabilities related to three areas:

- generally applicable regulations, in particular insofar as they regulate the operation of the national system for counteracting money laundering and financing of terrorism,
- the operation of the economy, and in particular the business practices of financial and non-financial institutions offering products and services that are associated with the risk of money laundering and financing of terrorism; in this area, it is important whether these institutions make every effort to mitigate this risk through the proper application of existing generally applicable legal regulations, as well as internal procedures in place in these institutions. This area also raises the issue of assessing whether the supervision exercised over the aforementioned financial and non-financial institutions is adequate,
- ways to counteract and combat cases of money laundering and financing of terrorism under the national system for counteracting money laundering and financing of terrorism.

Some of these vulnerabilities are currently being eliminated by implementing the AML/CFT strategy. Moreover, some of them (that are common to the entire EU) are covered by the legislative process in the EU regarding the so-called EU package.

517. In May 2021, *Resolution No. 50 of the Council of Ministers of 19 April 2021 on the adoption of the strategy for counteracting money laundering and financing of terrorism* was published (Monitor Polski (Official Gazette of the Government of the Republic of Poland) of 2021, item 435). It sets out an action plan aimed at reducing the risk related to money laundering and financing of terrorism. The actions to be implemented include, among others, ones related to legal regulations, such as:

(1) supplementing the list of obligated institutions in accordance with the proposals contained in the National Risk Assessment (this concerns mainly crowdfunding service providers);

(2) analysis of the legitimacy of amending the regulations regarding making or receiving payments in cash, concerning the effects of introducing a threshold for the amount of cash transactions for natural persons and enterprises;

(3) updating the regulations regarding virtual currencies, including the extension of their definition, based on the FATF standards for virtual assets;

(4) review of the legal regulations relating to associations and foundations to propose, if required, amendments thereto to enable competent authorities to exercise effective supervision over them;

(5) development of a proposal to amend the provisions regarding the rules for sector-specific supervision (non-financial sector) – concerning the verification of the commitment of obligated institutions to comply with the provisions on counteracting money laundering and financing of terrorism;

(6) introduction of clear regulations concerning off-site controls carried out by the GIFI in obligated institutions;

(7) re-initiation of work on the draft act amending the act – Foreign Exchange Law and the *Act on payment services*, providing for sector-specific supervision over online currency exchange platforms and adapting the rules of control over entities conducting currency exchange activities to control exercised over other entities from the financial sector (among others, with respect to the waiver of the obligation to inform the controlled entity about an intended inspection);

(8) implementation of the provisions of *Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 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* (OJ L 186, 11.07.2019, p. 122), hereinafter referred to as "Directive 2019/1153";

(9) completion of work on the implementing regulations and electronic document templates referred to in Articles 79, 84, 93, 94 and 109 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, as well as their implementation;

(10) development of a proposal to amend the regulations on the exchange of customer information between obligated institutions, as well as between obligated institutions and law enforcement agencies, supervisory authorities, the National Revenue Administration and the FIU, while maintaining the security of the exchange of this information – enabling the conclusion of bilateral agreements between obligated institutions, under which information will be exchanged between them with the mutual consent of the institutions involved;

(11) development of the concept of amending the legal regulations on the introduction of the obligation to keep a record book for monuments accepted or offered for sale (Article 59a of the *Act of 23 July 2003 on the protection and maintenance of historical monuments*) (Journal of Laws of 2022, item 840) in electronic form.

518. Many of the above actions concern the preparation of relevant legal acts or amendments to existing legal provisions (or the concept of such amendments). Their adoption and implementation should facilitate the prevention of money laundering and financing of terrorism, and – in some cases – harmonise Polish regulations with EU regulations and international rules. However, some of the above actions require – due to the complexity of the issues to which they refer – additional analyses with a view to possible adaptation of legal regulations.

519. Pursuant to the *Act of 1 December 2022 on the financial information system* (Journal of Laws of 2023, item 180), the legislator decided to create a Financial Information System (FIS) for collecting, processing and sharing information on open and closed accounts (i.e. bank accounts, accounts with cooperative savings and credit unions (SKOK), payment accounts with other entities, securities accounts and omnibus accounts, as well as cash accounts used to handle the accounts referred to in the two previous categories), as well as agreements on the provision of safe deposit boxes.

520. Information on accounts is collected primarily to combat phenomena of an international nature and reach that are exceptionally dangerous to the security of the state and citizens. The most serious cases related to money laundering disclosed in recent years have shown that the occurrence of irregularities in the area of counteracting money laundering can undermine the stability of the entire financial sector in a given country. The instability of the financial market may result in a threat to the financial security of the state and its citizens. Financing of terrorism is an international phenomenon. A given country may be of key importance for the financing of terrorism due to the use of the financial sector of that country in the chain of transactions related to this illegal practice. Due to the above, it is necessary to adopt regulations that guarantee quick and efficient obtaining of information on accounts kept for persons and entities associated with serious crime.

521. *The Act on the financial information system* also provided for certain amendments to the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, aimed at transposing the provisions of *Directive 2019/1153* into the Polish legal system, aimed at, among others:

- introducing the definition of financial analysis, operational analysis and strategic analysis, which will allow for the systematisation of work related to establishing methods of operation aimed at disclosing money laundering and terrorism financing trends and patterns, introducing an operating method/procedure – which defines the concept of strategic analysis and the determination of the outcome of a previously undertaken action/procedure, constituting a financial analysis,
- defining financial information for the purposes of determining the scope of information to be exchanged,
- introducing regulations regarding businesses operating on the non-bank market, providing safe deposit boxes, by introducing the definition of a safe deposit box, which aims to dispel doubts regarding the obligations arising from the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*,
- improving mechanisms aimed at ensuring a correct and effective channel of information exchange between the GIFI and law enforcement agencies,

- defining the requirements for communication systems used in communication with EUROPOL,
- the need to introduce relevant registers of requests for information that must be recorded in connection with the provision of financial information and analyses by financial intelligence units, as well as in connection with the exchange of information with EUROPOL.

522. The Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 included comments regarding the scope of sanctions that may be imposed on natural persons. The presented comments indicate the need to analyse the applicable provisions in order to take action to verify the fulfilment of the criterion of proportionate and dissuasive nature of penalties required by international standards.

523. The Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 also included comments regarding the powers of supervisory authorities:

- "there is no power to suspend a licence nor to require an obligated institution to take action",
- "not all supervisors are empowered to compel the production of information to reporting entities".

524. The aforementioned comments presented in the Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 indicate the vulnerability of the national system for counteracting money laundering and financing of terrorism that boils down to the lack of sufficient powers of the authorities supervising obligated institutions, which makes supervisory activities less effective.

525. Additionally, in relation to the money and value transfer services sector, the Report indicates that "there are no sanctions available for those MVTS which do not require authorisation but only need registration".

526. In terms of risk assessment and the application of a risk-based approach, the Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 indicated, among others, for the following gaps:

- "obligated institutions are not required to take into account the higher risks identified in the NRA or to incorporate information on those risks into their risk assessments,
- there is no requirement that the risk assessment conducted by the obligated institutions should be consistent with the country's assessment of its ML/FT risks,
- there is no requirement that the risk assessment conducted by the obligated institutions should be in line with the country's assessment of its ML/FT risks,
- the requirement for the obligated institutions to make their ML/FT risk assessments available to professional self-regulatory bodies or associations is discretional,
- there is no explicit requirement to take enhanced measures to manage and mitigate the risks where higher risks are identified,
- (…) supervision is not fully risk-based".

527. With regard to supervision over financial institutions, the Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 indicates that:

- "there is no written policy or procedure in relation to the frequency of review assessment of a FI's risk rating".

528. Moreover, in the Moneyval *Fifth Round Mutual Evaluation Report* from December 2021, attention was drawn to issues regarding politically exposed persons, in relation to whom it was indicated that:

- "the obligation to establish the source of the customer's wealth and sources of assets is limited to the customer and doesn't extend to BO,
- the definition of co-workers is narrower than the FATF definition of close associates,
- a direct reference to consider making a suspicious transaction report in case of life insurance contracts is absent".

The definitions of a politically exposed person, a family member or a person known to be a close associate of a politically exposed person adopted in the *Act on counteracting money laundering and financing of terrorism* transpose into the national legal system the analogous definitions contained in *Directive 2015/849*. Therefore, the comments included in the Moneyval Report point in fact to definitional differences between the FATF Recommendations and European Union law. Nevertheless, the comments from the aforementioned Moneyval Report indicate the potential vulnerability of the national system for counteracting money laundering and financing of terrorism, consisting in an insufficiently broad definition of concepts regarding the group of persons related to politically exposed persons. It is therefore necessary to consider the admissibility of amending the scope of the definitions contained in the *Act on counteracting money laundering and financing of terrorism*, covering the group of persons related to politically exposed persons, in order to take into account the scope of the definitions contained in the FATF Recommendations, while respecting the provisions of *Directive 2015/849*.

529. As regards comments concerning beneficial owners, the Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 indicates that:

- "it is possible for beneficial ownership information not to be complete for all associations, foundations and cooperatives within the totality of the system",
- "there is no legal, explicit, requirement for trustees or other persons involved with legal arrangements to disclose their status to obliged entities",
- "for cooperative savings and credit unions, there are no requirements in relation to beneficial owners, legal owners or management below the level of the management board, or in relation to associates of criminals".

530. The Moneyval *Fifth Round Mutual Evaluation Report* from December 2021 also indicates that in the *Act on counteracting money laundering and financing of terrorism*: "there is no provision clearly requiring obliged institutions to take steps to satisfy themselves that data and other relevant information relating to the understanding of the nature of the business will be made available by the third party without delay".

531. Eliminating the imperfections of the system requires undertaking relevant legislative work to adapt the regulations to the requirements indicated in the Report, which will ensure the

tightness of the system for counteracting money laundering and financing of terrorism, making it more effective.

532. On 20 July 2021, the European Commission adopted the AML Package of legislative proposals to strengthen the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules:

- AML/CFT Regulation (AMLR); *Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing* (OJ L 309, 25.11.2005),
- *AML/CFT Directive (AMLD6); Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law* (OJ L 284, 12.11.2018, p. 22),
- Regulation establishing a new EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLAR),
- Transfer of Funds Regulation – an amendment to track the transfer of cryptocurrencies (TFR).

533. The French Presidency continued to lead the Council negotiations on the AML Package, initiated by the Slovenian Presidency.

534. The priority of the work of the Council led by France was the AMLAR that, in line with the Council conclusions of 5 November 2020, is to establish a new EU agency that will contribute to the harmonisation and coordination of AML/CFT supervision in the financial and non-financial sectors, while directly supervising high-risk and cross-border financial institutions and supporting cooperation between financial intelligence units. The French Presidency hoped to obtain a negotiating mandate on the most important part of the text by the end of its term. Particular attention was paid to the key elements of the AMLAR, namely the harmonisation of definitions and the precise determination of the group of entities covered by the Regulation. The Presidency also focused on technical issues related to internal control and requirements relating to supervision over groups of companies.

535. The four EC legislative proposals included in the AML Package are a response to the deficiencies of the EU AML/CFT system identified by the EC in its reports published in 2019. These reports analyse the operation of the EU AML/CFT system in the context of high-profile cases of alleged money laundering involving EU credit institutions.

536. Based on the collected material, three basic problems affecting the effectiveness of the AML/CFT system in the EU were identified, i.e.:

- insufficiently clear and consistent rules of operation (for both private entities and public institutions),
- inconsistent supervision over obligated institutions,
- insufficient cooperation and information exchange between financial intelligence units.

537. The draft AMLD6 provides for the further development and interconnection of registers of beneficial owners, as well as the further development and interconnection of registers of

payment accounts, bank accounts and safe deposit boxes, where citizens' personal data will be collected. This data will be protected by the relevant provisions of the Directive as well as the GDPR. Access to this information by relevant authorities or obligated institutions is crucial from the point of view of counteracting money laundering and financing of terrorism. Tightening and increasing the effectiveness of the EU AML/CFT system thanks to the new legal measures provided for in the Directive will allow for a more effective fight against organised crime, which will improve the living conditions of citizens and increase their trust in legal economic transactions and public institutions.

538. The new EU Anti-Money Laundering and Countering the Financing of Terrorism Authority (AMLA) is to be the central element of the EU AML/CFT regime. The main tasks of this Authority will include ensuring uniform supervision over obligated institutions in the EU and facilitating cooperation between financial intelligence units. Its most important powers will include direct supervision over financial institutions conducting cross-border activities and facing the highest AML/CFT risk. As regards national FIUs, the AMLA is primarily to act as a platform for their cooperation.

539. Its activities should improve the quality of AML/CFT supervision over obligated institutions in the EU and increase the effectiveness of joint analyses performed by FIUs. This should make the AML/CFT system in the EU more effectively protect the single market against abuse by criminals using it to launder money or transfer funds to terrorists. The main objective of the AML/CFT policy is to deprive criminal groups of their income that motivates them to engage in criminal activity and is necessary to maintain the organisation. Increased effectiveness of counteracting money laundering and financing of terrorism means greater security for EU citizens, which will also enhance their trust in legal economic transactions and the financial system.

540. When performing a vulnerability analysis, it should be noted that certain steps have been taken to improve the system over the years, e.g. an amendment to *Regulation of the Minister of Justice of 8 May 2001 on the framework scope of the report on the foundation's activities* (Journal of Laws of 2020, item 36). The amendment, that entered into force on 1 January 2019, introduced the obligation to include in the foundation's report information whether it is an obligated institution within the meaning of the provisions of the Act. Pursuant to point 11 added in Article 2 of the Regulation, in the report on its activities, the foundation must provide information on accepting or making by it a payment in cash as a single operation or several related operations, with a value equal to or exceeding the equivalent of EUR 10,000, indicating the date and amount of the operation. Moreover, pursuant to the added point 10 in Article 2 of the Regulation, the foundation is obliged to provide information whether it is an obligated institution within the meaning of the provisions of the Act.

541. At the same time, having regard to the fact that foundations may not show in their reports the links between particular financial operations, which makes it difficult to exercise control, they are obliged to indicate in their reports the form of obtaining revenue and incurring costs (e.g. cash, transfer), as well as information on the amounts deposited in payment accounts and in cash (amendment to Article 2(5) and (6) and (7)(f) of the Regulation). The introduced changes to the regulations enable the controlling entity to independently analyse the foundation's revenue and costs, among others, to determine the scale of cash payments accepted and made.

542. In order to thoroughly demonstrate inaccuracies or deficiencies in existing legal regulations that may be abused for the purposes of money laundering or financing of terrorism, the regulations should be analysed in the context of the experiences of the authorities concerned. They should include practical comments on how to improve regulations in order to improve the system.

543. Pursuant to Article 150(1)(3) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the administrative penalties include removal from the register of regulated activities, but there is no prohibition on conducting activity. In practice, the above may result in the fact that an entity affected by a sanction in the form of removal from the register will be able to re-register by submitting an application, e.g. for entry in the register of currency exchange office operators, which will only involve payment of approx. PLN 1,000. Therefore, for this sanction to be effective, it is reasonable to consider extending its scope to also include a ban on conducting business activity, which would limit the possible circumventing its effectiveness.

544. Having regard to the reservations raised in the report on the implementation of *Directive 2015/849*, as well as the problems and limitations arising in the ongoing information exchange process, the following issues that may require legislative intervention should be indicated:

- introduction of the obligation to provide feedback about the use made of the information provided in response to a request submitted to the GIFI pursuant to Article 105(1) and (4) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*,
- introduction of additional provisions regarding the secrecy of financial information, in particular the handling by the prosecutor of the aggrieved party's motions as to evidence, as part of a request for information and the subsequent disclosure of the information obtained to the aggrieved party,
- harmonising the content of Article 83(3) with the content of Article 81(4) of the aforementioned Act,
- adapting the content of Article 104(2) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* to the needs related to information exchange between the GIFI and the prosecutor's office.

545. It should be noted that some of the statutory delegations provided for in the *Act of 1 March 2018 on counteracting money laundering and financing terrorism* have been failed to be implemented, which results in incompleteness of the regulations regarding the system for counteracting money laundering and financing of terrorism and may impair the accuracy of its operation:

- pursuant to Article 79(3), the minister competent for public finance shall determine, by way of a regulation, the method of preparing and submitting the notification referred to in Article 74, as well as the information and documents referred to in Article 76 and the procedure for their transfer, having regard to the need to ensure their efficient, reliable and secure transfer,
- pursuant to Article 84(4), the minister competent for public finance shall determine, by way of a regulation, the method of preparing and submitting, using electronic

means of communication, the information referred to in Article 81, as well as the notifications referred to in Article 83 and the procedure for their transfer, having regard to the need to ensure their efficient, reliable and secure transfer,

- pursuant to Article 94, the minister competent for public finance shall determine, by way of a regulation, the method of preparing and submitting:
  - notifications referred to in Article 86(1) and Article 90(1),
  - confirmations referred to in Article 86(3),
  - requests referred to in Article 86(5) and Article 87(1),
  - exemptions referred to in Article 86(6),
  - notification information referred to in Article 89(8),
  - and the procedure for their transfer, having regard to the need to ensure their efficient, reliable and safe transfer.

546. The regulation referred to in Article 109 of the aforementioned Act, regarding the preparation and acceptance of the requests referred to in Articles 104 and 105, and the provision of information referred to in Article 106, has not been adopted either. However, the adoption of this regulation is optional.

547. It should be emphasised, however, that pursuant to Resolution 50 of the Council of Ministers of 19 April 2021 on the adoption of the strategy for counteracting money laundering and financing of terrorism (Journal of Laws of 2021, item 435), in Priority IV regarding optimisation of the procedure, scope and quality of information exchange and access to information, Measure 15 provided for the completion of work on the implementing regulations and templates of electronic documents referred to in Article 79, Article 84, Article 93, Article 94 and Article 109 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* until the end of 2022.

548. In reference to the above, the aspect of the exchange of information regarding the proper performance of obligations arising from the Act between the GIFI and obligated institutions needs to be mentioned. The presentation of interpretations of statutory regulations by the GIFI facilitates the adoption of a uniform interpretation of the regulations, which may be important for improving the quality of performance of their statutory obligations by obligated institutions.

549. It should also be noted that the failure to indicate a donation as a form of settlement in the provisions of the Act may result in attempts to use donations to hide actual money transfers in order to circumvent the regulations on counteracting money laundering and financing of terrorism.

550. National regulations do not clearly regulate forfeiture of funds to the State Treasury where in the course of criminal proceedings in which the notification concerned an offence under Article 299 of the *Penal Code*, the proceedings have been discontinued due to the failure to detect the perpetrator. In such cases, prosecutors apply the provisions of the *Act of 18 October 2006 on the liquidation of unclaimed deposits* (Journal of Laws of 2006, No. 208, item 1537).

551. Article 299 of the *Penal Code* provides for liability for an act committed intentionally, which means that persons commonly classified as "straw men" may avoid liability for participation in activities involving money laundering. A natural person who provides their data

for remuneration where a bank account is opened using this data to be used for money laundering, will not be held liable under Article 299 of the *Penal Code* if there is no evidence that they acted intentionally.

552. The current wording of Article 2(1)(16)(c) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* results in interpretative doubts regarding the group of entities subject to obligatory entry in the register specified in Article 129a(1) of the aforementioned Act. According to selected entities making comments regarding the NRA, it is reasonable to make this provision more specific so that its interpretation does not raise doubts. According to the GIFI, the content of the provision of Article 2(1)(16) of the aforementioned Act corresponds to the general nature of the regulation and is similar to the solutions used in the draft EU regulations[253] in which general concepts are used as well.

553. Article 2(1)(15a) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* includes the phrase "primary activity", that has no definition in the Polish legal system. For the purposes of interpreting the aforementioned provision, it is reasonable to refer to concepts defined in an act, e.g. in the Act on the National Court Register that includes a definition of "predominant business activity". The concept of "predominant activity", despite the lack of a definition, can be reconstructed based on the judgements of administrative courts.

554. The amendment to the provisions governing the maximum period for suspending a transaction or blocking an account and to the provisions governing the seizure of property and real evidence is an important legal change that affects the shape and operation of the system for counteracting money laundering and financing terrorism. Until 11 January 2022, when the Act of 17 December 2021 amending certain acts in connection with the establishment of the Central Office for Combating Cybercrime (Journal of Laws of 2021, item 2447), hereinafter referred to as the "COCC Act", entered into force, the prosecutor could, by way of a decision, suspend a transaction or block an account for a period not longer than 6 months from the date of the notification. After the lapse of this period, the transaction suspension or the account blockade was waived, whereby some prosecutors issued (after the lapse of the suspension or blockade period) a decision to recognise the funds in the bank account as real evidence. Recognising funds in a bank account as real evidence was addressed by the Supreme Court in its resolution of 13 October 2021, I KZP 1/21, and in its resolution of 9 November 2021, I KZP 3/21. In the reasons for both resolutions, the concept of "real evidence" was analysed. It was pointed out that "funds deposited in a bank account do not have these features because they do not exist as things – items, they are only records in the IT system. It is an IT record with no corresponding item – a banknote that could be examined" (I KZP 1/21). In the reasons for both resolutions, it was also noted that it is permissible for the prosecutor to issue a decision regarding real evidence where the preparatory proceedings are in the *in rem* phase and no one has been charged. From 12 January 2022, after the COCC Act entered into force, the prosecutor may, by way of a decision, suspend a transaction or block an account for a period of 6 months that may be extended for another 6 months by way of a decision. At the same time, following an amendment to the provisions of the *Code of Criminal Procedure* by adding Article 236b thereto, the decision regarding real evidence may concern funds deposited in the account. On 18 May 2022,

[253] See Proposal for a *Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937* link https://www.consilium.europa.eu/pl/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

the Supreme Court issued a decision (I KZP 7/21) in which it reaffirmed that issuing a decision to recognise funds deposited in a bank account as real evidence is also admissible where criminal proceedings are in the *in rem* phase.

555. A legal problem noticed by the GIFI was the discontinuation of preparatory proceedings by the prosecutor's office due to the lack of national jurisdiction over acts committed via a bank account kept by a bank based in the Republic of Poland. This applies, for example, to those proceedings where the GIFI, pursuant to Article 86(8) of the *Act on counteracting money laundering and financing of terrorism*, notified the competent prosecutor of the suspicion of committing an offence involving money laundering or financing of terrorism. Some of the preparatory proceedings undertaken as a result of these notifications are discontinued under Article 17(1)(8) of the *Code of Criminal Procedure* due to the fact that, according to the authority conducting the proceedings, the perpetrator is not subject to Polish criminal courts' decisions. These grounds were invoked in several prosecutor's decisions in cases where the account used for suspicious activity was opened with a bank based in the Republic of Poland, but the real evidence showed that the transfer instructions were made via an IT system where the connection IP was other than Polish. These grounds for discontinuing preparatory proceedings in criminal cases of the type described above are inappropriate. Some of the GIFI's complaints against decisions to discontinue preparatory proceedings including the issue of national jurisdiction were acknowledged by the competent courts. In order to counteract this practice, that the GIFI finds erroneous, the GIFI files complaints against decisions that indicate the lack of national jurisdiction as the grounds for discontinuing proceedings, and has organised hybrid workshops for prosecutors regarding the issue of national jurisdiction. At the same time, the GIFI has entered into correspondence with the Ministry of Justice in order to prevent discontinuing preparatory proceedings regarding money laundering offences due to the lack of national jurisdiction.

556. Selected entities submitting their comments to the NRA pointed to a problem relating to receiving feedback by obligated institutions from the GIFI in connection with the activities taken by these institutions in the area of counteracting money laundering and financing of terrorism. This issue is very complex and its assessment presented by the GIFI differs from that presented by obligated institutions While the GIFI agrees that the provision of feedback in the analytical area, which is already partially provided for in the regulations, could be more extensive, its practical aspect should also be pointed out, namely that this would even more increase the tasks imposed on the GIFI and the organisational unit responsible for ensuring the proper implementation of the GIFI's tasks, given its very limited and overburdened resources.

557. Two vulnerabilities in the regulations regarding control are covered by legislative work at the level of the Ministry of Finance: the possibility for GIFI inspectors to present an inspection ID and authorisation to carry out an inspection on a remote basis, as well as the adequate application of selected provisions of the *Code of Administrative Procedure* to controls carried out by GIFI inspectors.

558. So far, there has been no provision regulating the activities of inspectors where it is not possible to present authorisation to carry out an inspection or an ID card. This problem was noticed and a relevant amendment consisting in adding paragraph 1a to Article 134 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* was provided for in the *Act of 16 August 2023 amending certain acts in connection with ensuring the*

development of the financial market and the protection of investors in this market (Journal of Laws of 2023, item 1723).

559. During an inspection in the area of counteracting money laundering and financing of terrorism, it is possible to verify compliance with all obligations in the AML/CFT area. However, not all possible types of violations of regulations in this area can be penalised. In particular, so far it has not been possible to impose a penalty for violating the obligation specified in Article 41(1) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, which significantly limited the inspection authorities' ability to respond appropriately in cases of failure to fulfil their obligations by obligated institutions. This problem was noticed and a relevant amendment to Article 147 of the aforementioned Act was provided for in the *Act on the Financial Information System*.

560. The lack of statutory regulations providing for a deadline for initiating proceedings to impose sanctions following a completed inspection increases the risk that violations identified as a result of the inspection will be barred by limitation.

561. Online currency exchange platforms that do not take possession of the customer's funds are still not subject to any requirements, which gives rise to a risk that this area will be used for money laundering.

562. Legal provisions do not regulate supervision over institutions obligated under Article 2(1)(12) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. Currently, there are only two requirements: no criminal record for the economic operator[254] and obligatory registration before starting business activity. These market entry barriers are very lenient, which makes a market area highly susceptible to money laundering and financing of terrorism accessible to everyone, including those who may want to use these obligated institutions to launder the proceeds of crime. This can also be observed as regards taking up business activities by foreign entities in Poland. Currently, it is possible for virtual currency service providers registered in countries whose AML systems differ significantly from those in force in the EU or EEA to operate in Poland.

563. From the point of view of the susceptibility of obligated institutions to threats related to money laundering and financing of terrorism, it would be advisable for them to be covered by an independent audit function. However, not all financial institutions have been covered by provisions regarding an independent audit function to verify their compliance with system for counteracting money laundering and financing of terrorism. As a result, some obligated institutions may be more susceptible to being used for money laundering than other obligated institutions with a very similar business profile.

564. Foundations, as obligated institutions, are obliged to submit annual substantive reports on their activities and financial statements. Failure to submit a substantive report does not entail any sanctions for the foundation. This issue has been raised, also in the doctrine[255], as a deficiency in the provisions regulating the operation of foundations. Therefore, it seems reasonable to introduce sanctions for foundations that fail to submit reports and to extend the supervisors' powers with respect to foundations to include, in particular, those that will make

[254] This applies to a sole trader or partners/managers of organisational units and the beneficial owners of the economic operator.
[255] Cf. Commentary to Article 12 in G. Gura, Ustawa o fundacjach. Komentarz, Warsaw, 2021

it possible to determine whether a given foundation is still operating and, if so, whether it can be considered an obligated institution.

565. There are also gaps in the legal regulations regarding associations. Also in this case, supervisors' powers should be extended to include, in particular, those that will enable them to determine whether a given association is still operating and, if so, whether it can be considered an obligated institution.

566. The Office of the Polish Financial Supervision Authority is authorised to participate in colleges of supervisors dedicated to counteracting money laundering and financing of terrorism organised by EU AML supervisors. Participation in such colleges has been provided for by the *Act on the Financial Information System* that entered into force on 10 February 2023. On 6 September 2023, the first AML/CFT college organised by the Office of the Polish Financial Supervisory Authority for the PKO Bank Polski S.A. Group was held.

567. As regards the GIFI's educational activities, it is worth noting that the GIFI has undertaken to publish two newsletters that can be read by obligated institutions following their registration on the GIFI website.

568. Summing up, it should be noted that major threats to the stability of the system include legal loopholes as well as the lack of uniform interpretation of regulations that, in the event of irregularities in the implementation of directives, could be an effective tool to enhance the proper application of regulations, also taking into account legislative omissions that significantly affect the operation of the system whose legal framework is based on national regulations. A uniform interpretation of legal provisions could be based on interpretations issued by the GIFI.

7.2. VULNERABILITY OF THE MARKET

569. ML/FT risks can be divided into two types, i.e. those occurring in the financial market and others that refer to the non-financial area. It should also be noted that both types of markets are interconnected, in particular when entities offer their services or products outside the financial market.

570. Some risks are common to all entities, both those operating in the financial market and outside it. Particular attention should be paid to the risk of using the employees of these entities by criminals to help them in laundering money and financing terrorism, and to these entities' involvement in blending income from legal sources with illicit proceeds.

7.2.1. Vulnerability of the financial market

571. In the second half of 2021[256], the GIFI, as part of the review of the National Assessment of the Risk of Money Laundering and Financing of Terrorism (the previous document was prepared in July 2019), requested obligated institutions as well as the supervisory authorities, i.e. law enforcement agencies and other cooperating units, to complete online surveys (their content depended on the types of institutions completing them). The surveys were posted on the secure website of the GIFI in order to collect a range of information for the analysis of

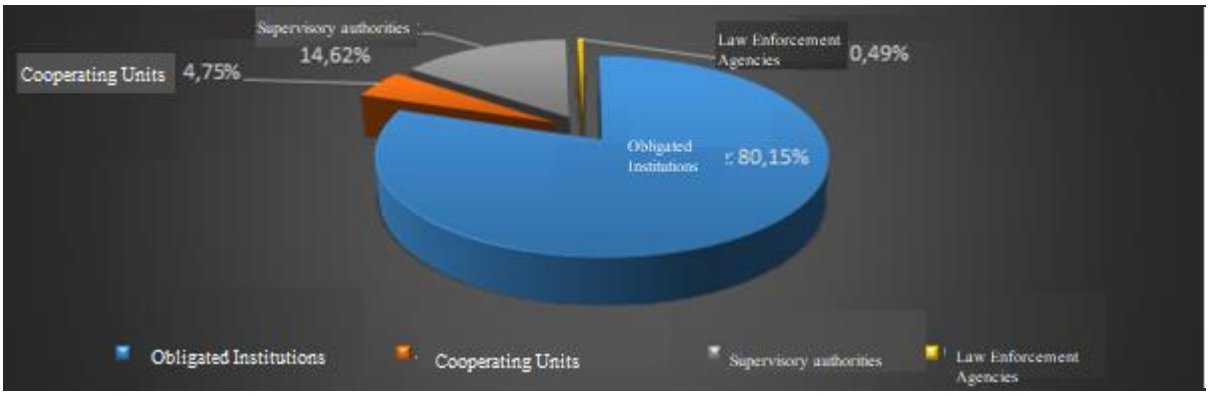
[256] in August 2021

various areas relating, directly or indirectly, to issues related to counteracting money laundering and financing of terrorism.

572. A total of 821 entities[257] responded to the surveys (compared to 263 responses received by the GIFI in 2019). A significant increase in the number of responses from particular entities and institutions resulted primarily from the form and method of survey completion (online). Most of the responses (658) came from obligated institutions.

573. The surveys were completed by persons representing particular entities, based on their knowledge and experience as well as information available in a given entity.

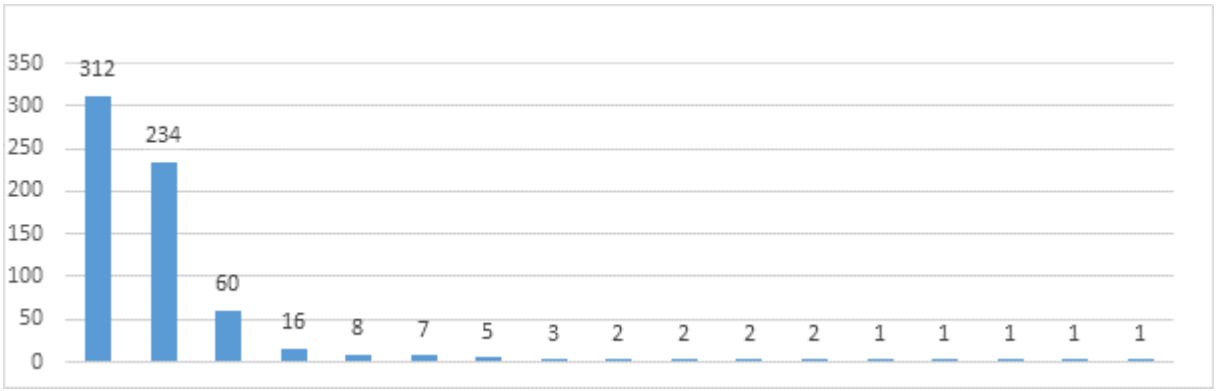
Chart 6. Breakdown of survey responses by entity categories



574. Based on their responses, it is known that approx. 80% of the completed surveys came from obligated institutions

575. (658). The share of particular obligated institutions in the survey concerned is presented in Chart 7 below.

Chart 7. Breakdown of responses to the surveys by categories of obligated institutions and the number of responses submitted by each category of obligated institutions



576. The largest number of survey responses were submitted to the GIFI by the following obligated institutions (7 categories of obligated institutions):

- currency exchange offices – 312 survey responses,

[257] compared to 263 responses in the surveys collected by the GIFI in 2019

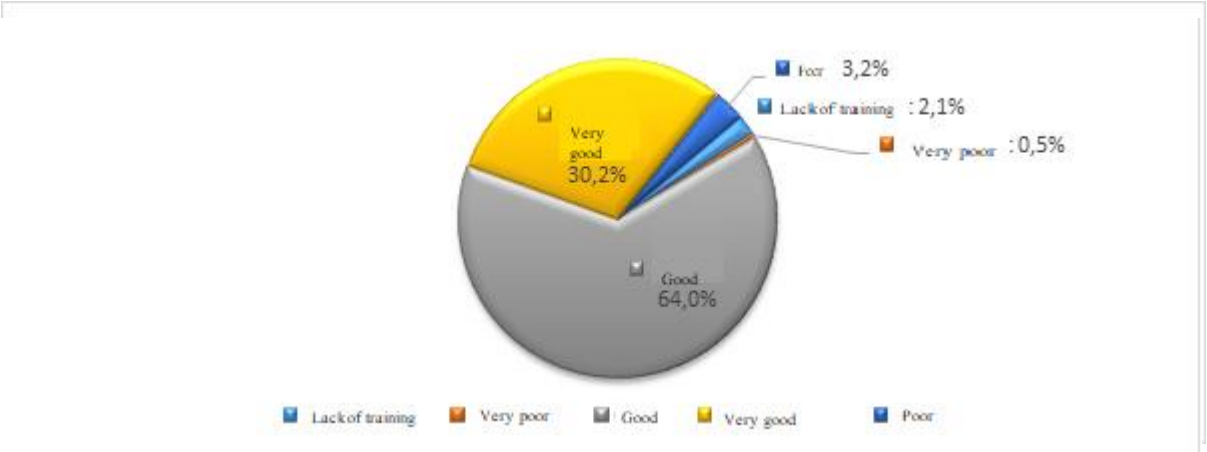
- banks – 234 survey responses,
- notaries – 60 survey responses,
- investment funds – 16 survey responses,
- economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law* – 8 survey responses,
- investment companies, custodian banks – 7 survey responses,
- domestic payment institutions, domestic electronic money institutions – 5 survey responses.

577. The other obligated institutions that submitted survey responses to the GIFI included, according to the data presented in Chart 7, cooperative savings and credit unions and the National Association of Cooperative Savings and Credit Unions (3 survey responses), insurance companies (2 survey responses), entities conducting business in the field of games of chance, betting, card games and games on gaming machines (2 survey responses), tax advisors (2 survey responses), notaries – with respect to the activities referred to in Article 79(6a) of the *Act of 14 February 1991 – Law on Notaries* (2 survey responses), economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, insofar as they accept or make payments for goods in cash with a value equal to or greater than the equivalent of EUR 10,000 (1 survey response), postal operators (1 survey response), economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, who are not other obligated institutions (Article 2(1)(16) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*) (1 survey response), lawyers, legal counsels, foreign lawyers, tax advisors (1 survey response), virtual currency exchange service providers (1 survey response).

578. According to the information contained in the survey for obligated institution, 644 persons out of 658 who completed it (97.9%) participated in AML/CFT training. Based on the information contained in the survey responses, it was established that persons who did not participate in the aforementioned training (2.1%) represented the following obligated institutions: currency exchange offices (7 entities), economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law* (5 entities) and notaries with respect to activities performed in the form of a notarial deed (2 entities).

579. In their responses, obligated institutions also referred to the level of AML/CFT training. Opinions in this regard are presented in the chart below.

Chart 8. Breakdown of responses to the surveys by categories of obligated institutions



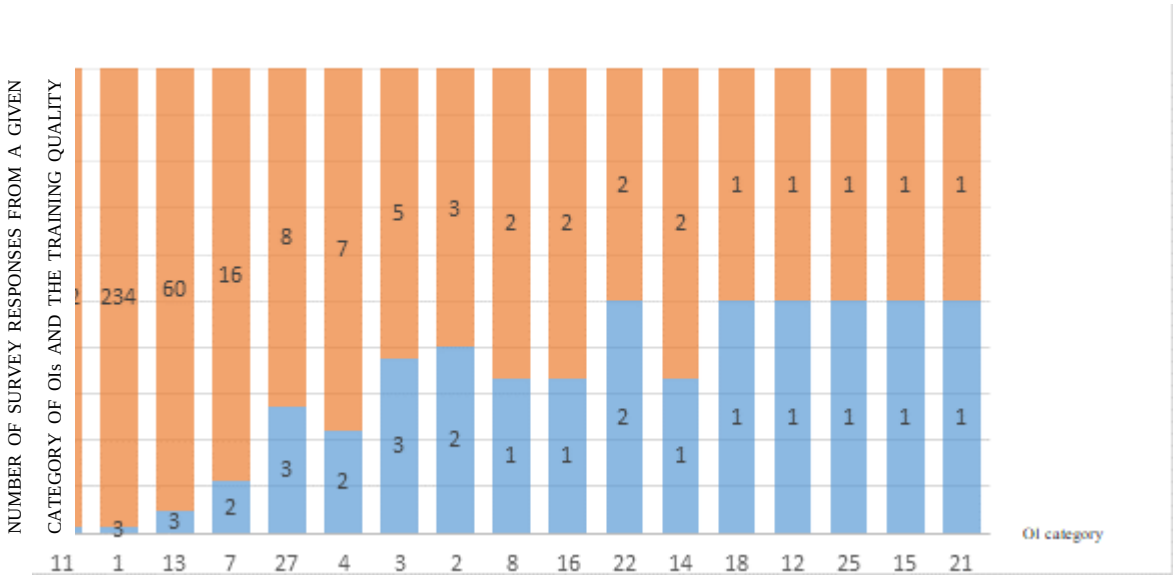
580. In the vast majority of the responses in this regard, the conducted training was assessed as very good (199 responses, 30.2%) or good (421 responses, 64.0%) – a total of 620 responses (94.2%). A small number of the responses referred to the lack of training (14 entities) and its very poor or poor quality – 3 entities and 21 entities, respectively.

581. The distribution of particular responses according to the assessment (scale from 1 to 4[258]) of the training and the category of obligated institutions[259] (OI) is presented in the chart below.

Chart 9. The number of survey responses from particular categories of obligated institutions (orange) and the training quality according to particular obligated institutions (blue)

[258] Quality of the conducted training (blue colour in Chart 9): 4 - very good, 3 - good, 2 - poor, 1 - very poor

[259] 11-currency exchange offices, 1-domestic banks, branches of foreign banks, branches of credit institutions, financial institutions having their registered office in the territory of the Republic of Poland and branches of financial institutions that do not have their registered office in the territory of the Republic of Poland, 13-notaries – with respect to activities performed in the form of a notarial deed, 7-insurance companies, 27-economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, conducting business activities consisting in: (a) trading or intermediation in the trade of works of art, collectors' items and antiques within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services*, also where such activities are conducted: in art galleries or auction houses, 4-investment companies, custodian banks within the meaning of the *Act of 29 July 2005 on trading in financial instruments*, 3-domestic payment institutions, domestic electronic money institutions, branches of EU payment institutions, branches of EU and foreign electronic money institutions, small payment institutions, payment service providers and clearing brokers, within the meaning of the *Act of 19 August 2011 on payment services*, 2-cooperative savings and credit unions and the National Association of Cooperative Savings and Credit Union, within the meaning of the Act of 5 November 2009 on cooperative savings and credit unions, 8-insurance companies carrying out the activities referred to in Section I of the Annex to the *Act of 11 September 2015 on insurance and reinsurance activities*, 16 -tax advisors with respect to tax advisory activities other than those listed in Article 2(14) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* and expert auditors, 22-entities conducting business involving games of chance, betting, card games and games on gaming machines, within the meaning of the *Act of 19 November 2009 on gambling*, 14-notaries – with respect to the activities referred to in Article 79(6a) of the *Act of 14 February 1991 –Law of Notaries*, 18-economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, that are not other obligated institutions (Article 2(1)(16) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*), 12-entities conducting business activities involving the provision of services in the field of: exchange between virtual currencies and legal tenders, exchange between virtual currencies, 25-economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, insofar as they accept or make payments for goods in cash with a value equal to or exceeding the equivalent of EUR 10,000, 15-lawyers, legal advisors, foreign lawyers, tax advisors, 21-postal operators within the meaning of *Act of 23 November 2012 – Postal Law*.



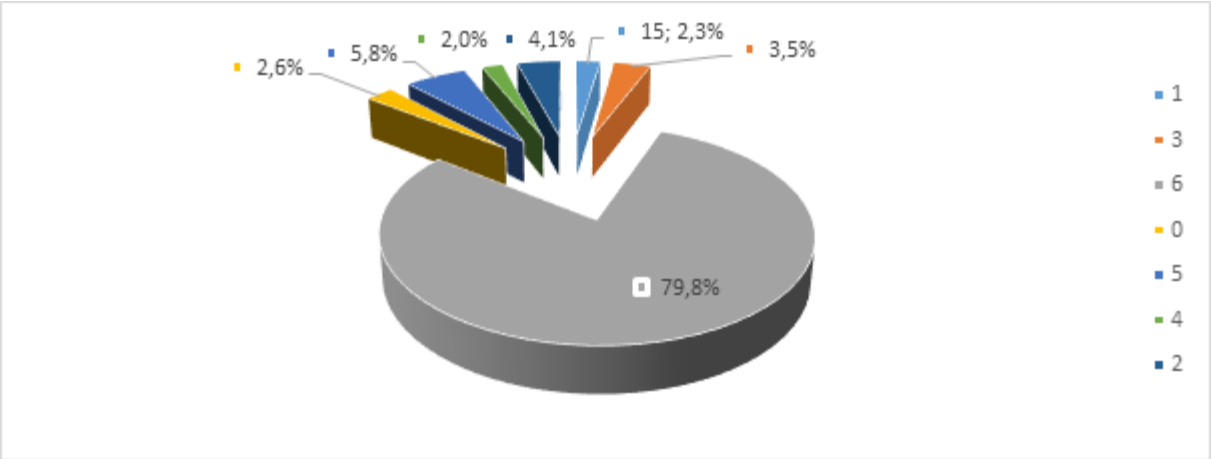
582. Based on the survey, the largest number of training courses (142) were conducted in July 2018 – May 2021 – in accordance with the results of the survey responded to by 443 obligated institutions. The indicated period resulted from the dates relevant to the transposition of *Directive 2015/849* of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing into the Polish legal system and amending the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*[260].

583. According to the responses provided by obligated institutions, 525 persons completing the survey on behalf of obligated institutions, i.e. approx. 79.8%, had been dealing with counteracting or combating crime (including counteracting money laundering and financing of terrorism) for more than 5 years. The numbers under Chart 10 stand for years of experience of the persons completing the survey, i.e.: 0 – 'less than one year', 1 – 'for one year', 2 – 'for two years', 3 – 'for three years', 4 – 'for four years', 5 – 'for five years', 6 – 'for more than five years'.

Chart 10. Breakdown of survey responses by years of experience in counteracting or combating crime (including counteracting money laundering and financing of terrorism)[261]

[260] On 13 July 2018, the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* (the so-called 'new AML Act') entered into force. The Act implemented the provisions of 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 (commonly known as AMLD IV). On 14 May 2021, the AMLD IV was amended in the Polish legal system.

[261] 0 – 'less than one year', 1 – 'for one year', 2 – 'for two years', 3 – 'for three years', 4 – 'for four years', 5 – 'for five years', 6 – 'for more than five years'.



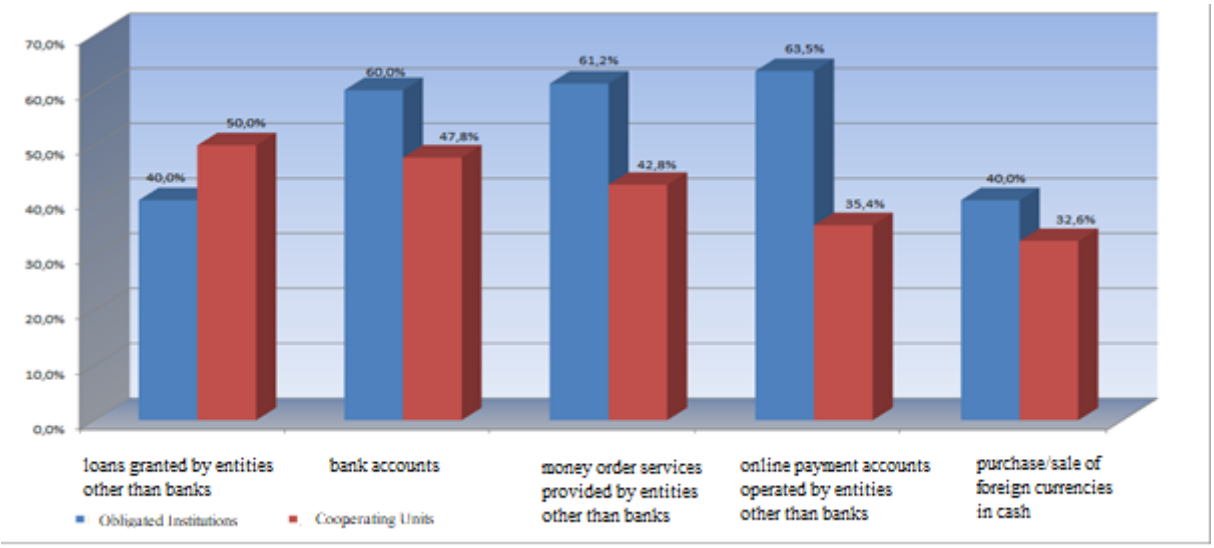
584. All types of the surveys included a request to indicate five products and services offered in the financial market that are or can be most often used for money laundering. The responses were selected from a list containing the following items:

- bank accounts,
- loans and credits granted by banks,
- payment services provided by banks,
- money order services provided by entities other than banks,
- online payment accounts operated by entities other than banks,
- other payment services provided by entities other than banks,
- services provided as part of the underground banking system (e.g. Hawala),
- credit and debit cards,
- prepaid cards,
- virtual payment cards (e.g. for Mail Order & Telephone Order (MOTO) transactions),
- letters of credit,
- guarantees,
- collections,
- traveller's cheques,
- other cheques,
- bills of exchange,
- units in investment funds,
- securities,
- derivatives,
- leasing,
- 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 handle them,
- unit-linked life insurance,
- other financial products and services.

585. The list of five products and services indicated by the largest number of obligated institutions is the same as the list of five products and services indicated by the largest number of cooperating entities. The only difference is in their order. In the case of obligated institutions, the largest number of their responses concerned online payment accounts operated by entities other than banks, followed by money order services provided by entities other than banks, bank accounts, as well as loans granted by entities other than banks and purchase/sale of foreign currencies in cash. The responses of cooperating units show that the products and services used most frequently for money laundering include loans granted by entities other than banks, followed by bank accounts, money order services provided by entities other than banks, online payment accounts operated by entities other than banks, and purchase/sale of foreign currencies in cash.

Chart 11. Responses regarding products and services offered in the financial market that are most often used for money laundering



586. Summing up, both the cooperating units and the obligated institutions that provided their responses to the survey questions indicated that products and services used most often for money laundering included those related to virtual currencies, banking, payment services, currency exchange and loans. The threats related to these areas are described below.

Banking

587. Pursuant to Article 5(1) of the *Act of 29 August 1997 – Banking Law*, regarding *banking activities*, specific types of activities[262] may be performed exclusively by banks, although this does not mean that the range of products and services they offer is limited. A substantial part of the banks' offer is related to maintaining bank accounts.

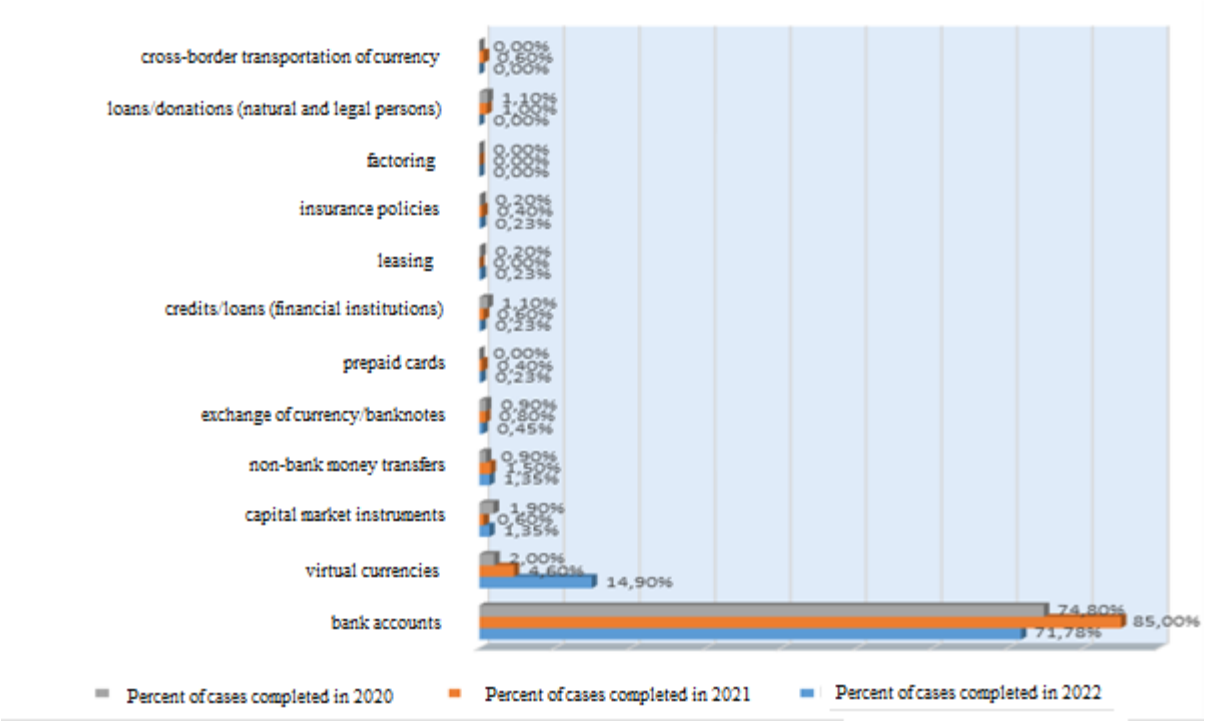
588. The analysis of information regarding the typology of conducted analytical proceedings[263] initiated by the GIFI in 2020-2022 (table below) shows that most of them concerned suspicions of money laundering or financing of terrorism in connection with the use of bank accounts for suspicious transactions (in 2020, such proceedings accounted for 74.8% of all analytical proceedings, in 2021 and 2022, these figures were 85.0% and 71.78%, respectively)[264].

Table 21. Typologies by category for 2020-2022

Typology name	Number of cases completed in 2022	Total number of cases completed in 2022	Percent of cases completed in 2022	Number of cases completed in 2021	Total number of cases completed in 2021	Percent of cases completed in 2021	Number of cases completed in 2020	Total number of cases completed in 2020	Percent of cases completed in 2020
Factoring	0	443	0.0%	0	526	0.0%	0	540	0.0%
Other	10	443	2.26%	7	526	1.3%	16	540	3.0%
capital market instruments	6	443	1.35%	3	526	0.6%	10	540	1.9%
prepaid cards	1	443	0.23%	2	526	0.4%	0	540	0.0%
loans/credits (financial institutions)	1	443	0.23%	3	526	0.6%	6	540	1.1%
Leasing	1	443	0.23%	0	526	0.0%	1	540	0.2%
insurance policies	1	443	0.23%	2	526	0.4%	1	540	0.2%
non-bank money transfers	6	443	1.35%	8	526	1.5%	5	540	0.9%
loans/donations (natural and legal persons)	0	443	0.0%	5	526	1.0%	6	540	1.1%
cross-border transportation of currency	0	443	0.0%	3	526	0.6%	0	540	0.0%
bank accounts	318	443	71.78%	447	526	85.0%	404	540	74.8%
virtual currencies	66	443	14.90%	24	526	4.6%	11	540	2.0%
currency/banknote exchange	2	443	0.45%	4	526	0.8%	5	540	0.9%

Chart 12. Completed analytical proceedings initiated by the GIFI in 2020-2022, broken down by products and services used for suspicious transactions (according to data as at 20 April 2023)

[262] That is: 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 banks in other acts.
[263] That is: concluded with the submission of a notification to the prosecutor's office or information to another authorised public administration body/unit in accordance with the AML/CFT provisions. Analytical proceedings were initiated based on information from both obligated institutions and cooperating units.
[264] According to the information on analytical proceedings, recorded in the GIFI IT system on 20 April 2023.



589. It is relatively simple to open a bank account and make transactions through it (including cross-border ones). It should be remembered that in the modern world, committing a predicate offence for money laundering often involves obtaining funds that are already present in non-cash transactions (e.g. from various types of fraud and deception).

590. The risk of money laundering and financing of terrorism related to bank accounts is mainly affected by their following features:

- ability to carry out cross-border transactions (i.e. ones carried out outside the country where the account is maintained),
- relatively quick transfer of funds,
- ability to make cash transactions (both to credit the account and to debit it),
- relatively quick and easy access to the bank account and the execution of transactions through this account via a telecommunications network (using the Internet, telephone lines),
- the ability to appoint account proxies who carry out transactions on behalf of its owner.

591. An important element of the offer is access to the account via electronic communication channels (in particular via the Internet) that make it easier to conceal the data of the actual payers (especially where "straw men" and "shell companies" are used for this purpose)[265].

[265] "Straw men" mean natural persons, while "shell companies" include only business entities, including natural persons running a business. What both categories of entities have in common is the purpose of their operation. In practice, straw men are random natural persons recruited by organised criminal groups in order to use their personal data to open a personal bank account or to establish a power of attorney to the account of another entity, or even to perform only one cash transaction (e.g. withdrawal of a large sum of money).

According to the NBP statistics[266], the total number of non-cash transactions is steadily increasing year on year. As at the end of 2022, their number exceeded 13.3 billion, while a year earlier, this figure was 11.35 billion (i.e. an increase of 17.06% between 2021 and 2022), whereby transfers[267] accounted for over 35.59% (in 2021) and 35.29% (in 2022) of the total number of non-cash transactions. As for transactions made using payment cards, these accounted for 64.15% and 64.49% of all non-cash transactions carried out in 2021 and 2022, respectively. The remaining value of non-cash transactions was attributed to financial operations carried out using cheques and direct debits.

592. Various additional services are often offered as part of maintaining bank accounts, including the collect service, i.e. mass payment identification. In general, the aforementioned service consists in enabling the bank's customer to generate numbers of virtual accounts (created in accordance with the NRB standard[268]) that in fact hide one settlement account of the bank's customer. As part of this service, the bank's customer is able to distribute these numbers among its trading partners in order to execute transactions for the bank's customer. The trading partner executes transactions for the bank's customer using a dedicated virtual account number or virtual account numbers. Transactions are, in fact, posted to the actual settlement account of the bank's customer.

593. The collect service – used increasingly often, not only by economic operators who have a large number of individual recipients of their products or services, but also by other entities – makes it difficult to analyse financial flows and identify the actual payer and payee of the transfer, in particular where information following from credit transfers or the records of the accounts of trading partners of the bank's customer is used. The service enables customers both to credit and debit a given. The accounting scheme and the scope of information provided to the bank often make it impossible to monitor and analyse transactions of particular customers on an ongoing basis and, where reasonable, to investigate the origin of assets at the disposal of a given customer. The collect service rendered to entities from the payment services sector generates a significant risk of money laundering, even though these entities are obligated institutions. Low barriers to enter the payment services sector combined with a high appetite for risk and acceptance of reputation loss indicate that due to the wide range of services that can be provided, entities in this sector may be used or even intentionally established by criminal groups to introduce assets originating from illegal or undisclosed sources into financial transactions.

594. Money laundering risks are also generated by loans and credits offered by banks. Apart from the possible use of "straw men" or "shell companies" to contract them and thus obtain money from banks under false pretences, i.e. committing a predicate offence for money laundering, they pose also other risks. First of all, loans and credits can be repaid with profits

[266] Report: *Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2022* r., NBP, April 2023, p. 52, Table 11, at: https://nbp.pl/wp-content/uploads/2023/05/Ocena-funkcjonowania-polskiego-systemu-platniczego-w-II-polroczu-2022-r.pdf

[267] 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 (source: Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2022 r., NBP, kwiecień 2023, p. 52, Table 11, at: Ocena-funkcjonowania-polskiego-systemu-platniczego-w-II-polroczu-2022-r.pdf (nbp.pl)).

[268] That is: the standard for the numbering of bank accounts in Poland (see provisions of Chapter IV of Ordinance 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)

from illegal sources. Moreover, funds from loans and credits may be transferred – as profits from legal sources – to third parties.

595. Prepaid cards are another product used in the Polish market that may generate money laundering risks[269]. The NBP analysed, among others, the prepaid cards market in Poland in Q3 2022[270]. As at the end of September 2022, the number of prepaid cards was 1.68 million, i.e. 279.4 thousand fewer than as at the end of June 2022 (a decrease by 14.3%). The share of prepaid cards in the market was 3.8% (as at the end of Q2, this figure was 4.5%).

596. Prepaid cards are classified primarily according to their purpose[271], i.e.:

- closed loop/semi-open loop prepaid cards,
- general-purpose prepaid cards, including: general purpose non-reloadable prepaid cards or general purpose reloadable prepaid cards.

597. The former may be used only to purchase goods or services in a specific store, chain of stores or shopping centre or, to purchase specified goods or services, regardless of the geographical location of the point of sale. Such prepaid cards include gift cards, e.g. issued by specific retail chains, membership cards, fuel cards to be used in a specific network of gas stations, and meal vouchers. Sometimes such cards are anonymous (especially in the case of gift cards). However, due to their limited use, the risks they pose are low.

598. General purpose prepaid cards have a wide range of applications. These cards can be used to pay salaries and various types of additional benefits for employees, as incentive cards or as cards used to settle expenses during business trips, as well as to pay social benefits, scholarships or pocket money, and to pay for goods bought online.

599. General purpose prepaid cards may be issued by banks or non-bank payment service providers, e.g. electronic money institutions. Prepaid cards may be either a scriptural (bank) money carrier and as such they are debit cards, or an electronic money carrier. Prepaid cards issued in Poland by domestic banks are only debit payment cards. They are a payment instrument linked, in principle, either to a standard payment account or to an account with limited functionality, i.e. used exclusively to handle payment orders executed through a card and to record funds credited to the account to cover future payment transactions. Data regarding this type of cards is reported to the NBP. The money laundering risks associated with prepaid cards issued by domestic banks is low – lower than in the case of traditional debit cards (due to limits on transactions, reloads or the total value of funds held on the payment instrument at any time)[272].

---

[269] Prepaid cards enable making payments using funds available in the payment account linked to the card. Before using the card, the account must be credited, e.g. through a credit transfer placed on the online banking website or by cash deposit at a bank branch.

[270] Report: Informacja o kartach płatniczych III kwartał 2022, posted on the NBP website at: https://nbp.pl/311738/, January 2023, p. 9.

[271] Based on the EC publication: 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.

[272] The lower risk compared to traditional debit cards results from the fact that prepaid cards are generally subject to stricter rules than debit cards. These rules are defined in a contract between the issuer-bank and the

600. The ability to issue anonymous prepaid cards (without identifying and verifying the customer) applies only to electronic money carriers, although there are certain limitations in this respect related to limits on the amounts held on the payment instrument, as well as limits on transaction amounts. The issuance of anonymous prepaid cards – electronic money carriers – in Poland is limited by the regulations provided for in Article 38 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. Currently, domestic banks do not issue prepaid cards that would constitute electronic money instruments.

601. Prepaid cards, including anonymous prepaid cards, are issued by foreign electronic money institutions offering their products and services on a cross-border basis in Poland under a European passport. These entities are subject to the supervision of their home country and have no reporting obligations towards the NBP regarding information on the number of cards issued and the volume of electronic money issuance, thus the scale of this activity is unknown. It is therefore difficult to assess the likelihood of the occurrence and the level of the risk of money laundering or financing of terrorism involving anonymous electronic money instruments in Poland. However, it should be borne in mind that EU AML/CFT regulations apply also in the countries of origin of electronic money institutions.

602. In order to ensure the development of prepaid cards and electronic money instruments in the Polish market, which would account for the need to ensure an adequate level of security of transactions carried out using such cards and instruments, in particular with respect to counteracting money laundering and financing of terrorism, the Payment System Council (a consultative and advisory body operating at the NBP Management Board) established a task force for prepaid cards in July 2018.The Task Force was to develop a proposal for a uniform approach to electronic money in the Polish market, as well as proposals for legislative, self-regulatory and educational and promotional activities necessary for the development of prepaid cards and electronic money instruments in the Polish market, ensuring an adequate level of their security. At its meeting held on 17 June 2019, the Payment System Council concluded that the Task Force for prepaid cards had achieved the objectives set out in the Council's resolution under which it was appointed and thus discontinued its operation. The Council then adopted recommendations[273] for actions related to the issuance and operation of prepaid cards and electronic money instruments in the Polish market.

603. Money laundering risks are also generated by credits and loans granted by banks, that can be used to commit a predicate offence for money laundering, in particular to deceitfully obtain money based on forged documents, and can also be used to launder money from illegal activities.

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, employer). Depending on the user (natural person or business entity) and the purpose for which the card is issued (e.g. payment of pocket money or salary, social benefit or business trip expenses), different types of restrictions may be imposed. These concern, e.g. the limit on one-time funds available on the card (in the case of a card linked to the parent's/business subaccount, usually lower than the balance of the payment account crediting 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 on non-cash and cash transactions.

[273] https://nbp.pl/system-platniczy/rada-ds-systemu-platniczego/komunikaty-rady-ds-systemu-platniczego/17-czerwca-2019/

604. Above all, loans and credits can be repaid using money coming from illegal sources. Collaterals may also be established on assets obtained illegally, that are then used to satisfy the bank's claims related to receivables resulting from the granted loan.

605. Another service provided by banks, that, however, is not reserved exclusively 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 profits from crime (in various forms, not just cash). As far as the risk of using this service for money laundering is concerned, it is important that banks are unable to objectively assess the type and actual value of items stored in safe deposit boxes.

Payment services

606. In the case of payment services, it is worth noting (among others) the growing values and numbers of transactions carried out by domestic payment institutions (DPI), small payment institutions (SPI) and payment service offices (PSO). According to the available information[274], the total number of transactions in the case of DPIs as at the end of Q4 2021 was 755.7 million compared to 575.2 million as at the end of Q4 2020. A steady increase in the volume of payment transactions between the particular quarters of 2021 (the number of transactions in Q1 2021 was 579.2 million, in Q2 2021 – 662.5 million) should also be noted. Most DPIs entered into the KNF register by 31 December 2021 meet the definition of a hybrid payment institution. This means that besides providing payment services, such entities also conduct other business activities[275]. The volume of payment operations carried out by small payment institutions (SPIs) in Q4 2020 – Q4 2021 increased by 0.15 million transactions. The situation of payment service offices (PSOs) is presented once a year, along with information on the situation of DPIs and SPIs for Q4 of a given reporting year.

Chart 13. Total number of payment transactions at DPIs (in million)

[274] Data from the KNF report: Informacja o sytuacji krajowych instytucji płatniczych, małych instytucji płatniczych w IV kwartale 2021 r. oraz biur usług płatniczych w całym 2021 r. (Information on the situation of domestic payment institutions, small payment institutions in Q4 2021 and payment service offices throughout 2021), p. 5, https://www.knf.gov.pl/?articleId=78002&p_id=18

[275] Ibidem, p. 4.

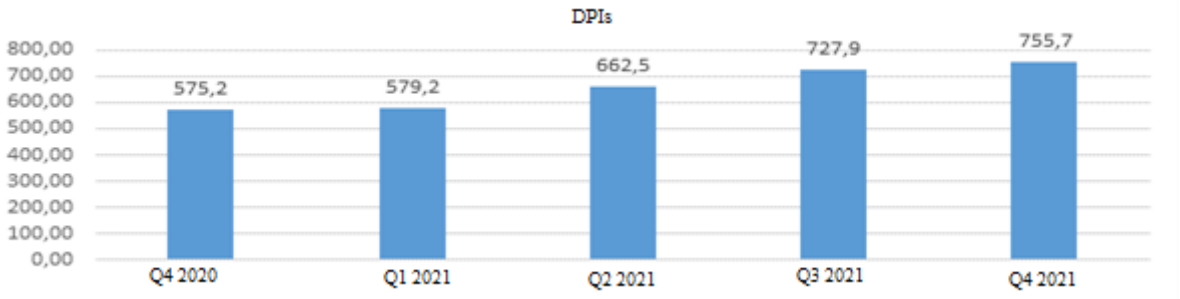
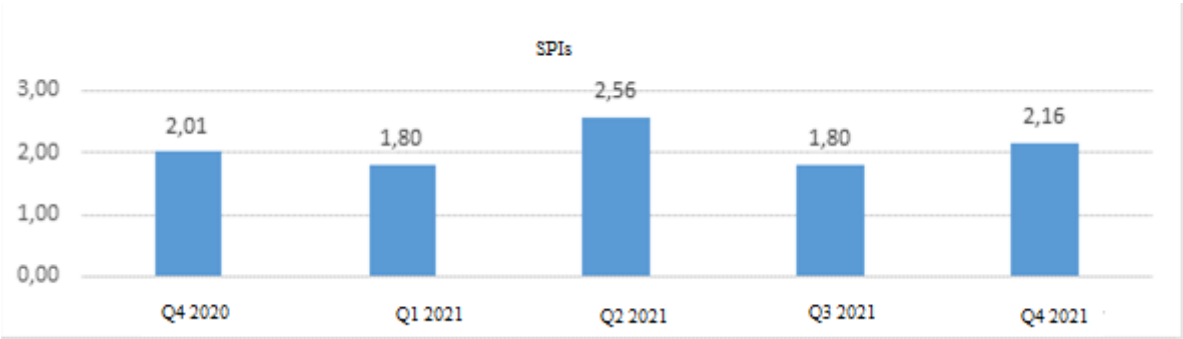


Chart 14. Total number of payment transactions at SPIs (in million)



607. A distinction is usually made between money order services, that 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 also be executed, e.g. depositing cash in order to transfer it on a non-cash basis to the payee's payment account and vice versa).

608. In Poland, money order services[276] are offered primarily by PSOs 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 order and money transfer services[277].

609. There are also entities offering only money transfer services via online platforms, often operating outside Poland or the EU. They can be used to transfer money to selected persons and entities, among others, to pay for purchases made online or participation in betting and gambling, also offered online. They also enable internal transfers between particular users of a given online platform. Foreign entities offering money transfer services via online platforms

[276] In accordance with Article 3(3) of the *Act of 19 August 2011 on payment services*, the money order service means "a payment service provided without any payment account being created in the name of the payee, consisting in the transfer of funds received from the payer to the payee or to another payment service provider acting on behalf of the payee, or in the receipt of funds for the payee and making them available to the payee".
[277] 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...".

sometimes hold accounts with Polish banks, through which they settle transactions ordered by their customers. Thus, ML/FT risks related to their activities are also transferred to those banks that make accounts available to them.

610. The risk of using non-bank payment services for money laundering is mainly related to their following characteristics:

- short time of payment transaction execution,
- ability to execute cross-border transactions between the payer and the payee staying in different countries,
- easy access – 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);
- quick access in the case of payment services offered by online platforms (7 days a week from anywhere in the world),
- ability to make transfers of payment services between particular users of a given online platform,
- lack of a proper warranty in the application of the AML/CFT regulations due to low opportunity costs resulting from reputation loss,
- lack of control over foreign payment service providers, in particular online platforms offering payment services operating outside the EU (limited possibilities of gaining access to information on their transactions and the identity of the actual payer and payee of the remittance).

611. Moreover, there is also a risk related to offering payment services by entities operating illegally, e.g. by using in these operations payment accounts kept on their behalf. This risk is generated, among others, with the operation of informal funds transfer systems, such as Hawala[278].

Currency exchange

612. Currency exchange is not a complicated service, although it can be carried out in several different ways. The basic one involves purchase and sale of convertible currencies in the cash form and is most often carried out by currency exchange office operators.

613. The activities of currency exchange offices in Poland are characterised by the fact that most of the transactions carried out are occasional, i.e. they are not carried out as part of business relationships.

614. Transactions concluded in the course of currency exchange activities as part of business relationships between the currency exchange office operator and the customer are rare.

[278] In this case, 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-FT.html).

615. The ML/FT risk related to such services is mainly due to the anonymity of occasional transactions that are often below the EUR 15,000 equivalent threshold, and the cash nature of the services offered.

616. Besides cash currency exchange services, cashless currency exchange services are also offered. They provide the opportunity to make transactions often at more favourable rates than in the case of cash exchange. These types of services are offered both by currency exchange office operators[279], banks or financial institutions, as well as by other types of entities. Online platforms enabling access to them are usually divided into online currency exchange platforms and peer-to-peer currency exchange platforms.

617. In the case of online currency exchange platforms, cashless currency exchange usually follows a similar pattern:

- the customer accepts the terms and conditions of the transaction, in particular the exchange rate, offered by the service provider,
- the customer transfers funds in one currency to the service provider's bank or payment account,
- the exchanged funds in another currency are transferred back by the service provider to the bank or payment account indicated by the customer.

618. Peer-to-peer currency exchange platforms match offers to buy and sell currencies submitted by particular customers, thus enabling them to make exchange transactions between them. However, the flow of funds takes place between the payment accounts of particular customers.

619. There are also online platforms for group currency purchases. Such platforms enable buying currencies at preferential rates used in the currency market. The platform is used to collect purchase orders for a given currency from its multiple users. The collected orders provide the basis for the execution of one aggregate transaction in the foreign exchange market. This allows for currency exchange at a more favourable rate than in the case of regular, "retail" transactions.

620. Sometimes – in the case of services offered by currency exchange office operators or banks – cash currency exchange is combined with cashless currency exchange. This is the case where, for example, the customer provides the service provider with cash to be exchanged with an instruction to transfer the exchanged money to the bank account indicated by this customer. The customer may also transfer money to be exchanged to the service provider's bank account and receive the exchanged funds in cash[280]. Payment cards may also be used to transfer money to be exchanged.

621. The aforementioned risks relating to the activities of currency exchange service providers also apply to cashless currency exchange services, including the risk of anonymous

[279] Cashless currency exchange via the Internet offered by entities providing currency exchange services is not a currency exchange activity within the meaning of the *Act of 27 July 2002 – Foreign Exchange Law* and is carried out outside this activity.

[280] In the case of currency exchange activities, transactions with the use of bank accounts shall be permitted only with respect to domestic currency settlements on account of foreign currency cash exchange at a currency exchange office.

transfer of assets to third parties (e.g. by indicating by the customer a bank account or another payment account belonging to third party (claiming that it is this customer's account) to which the service provider is supposed to transfer the exchanged funds).

622. It is also worth noting that entities operating online platforms for cashless currency exchange sometimes offer additional services available on these platforms, such as purchase and sale of virtual currencies or trading in the Forex market.

Virtual currencies

623. The development of products and services that can compete with traditional financial products and services also takes place outside the financial market. Their development has been facilitated by the rapid progress of information technologies, as well as the ongoing digitalisation of society and the development of Internet access networks.

624. Entities conducting business involving virtual currencies are a group of economic operators conducting unregulated activities – operating outside the financial market – mainly under the provisions of the *Act of 6 March 2018 – Economic Operators' Law*. Virtual asset service providers (VASP) include obligated institutions indicated in Article 2(1)(12), (15a), (16)-(18), (23)-(24) and (24a) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*.

625. The concept of virtual currencies is defined in 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.

626. According to information from coinmarketcap.com[281], as at 30 June 2023, there were approx. 10,000 cryptocurrencies available. Due to the different form of source codes and the saved functionality of particular cryptocurrencies, each of them may generate different risks to the security of financial transactions. First of all, attention should be paid to cryptocurrencies that offer full anonymity and generate risk related to the ability to identify wallet addresses of a given cryptocurrency (e.g. Monero, Z-cash), and at the same time encrypt other information about the transaction, which ensures full anonymity of the payer and the payee.

627. The analysis of data on the capitalisation of virtual currencies (table below), presented by coinmarketcap.com[282], shows that Bitcoin /BTC/ continues to have the largest share in this market (approx. 50.1%). A significant share of Ethereum should also be noted (19.1%).

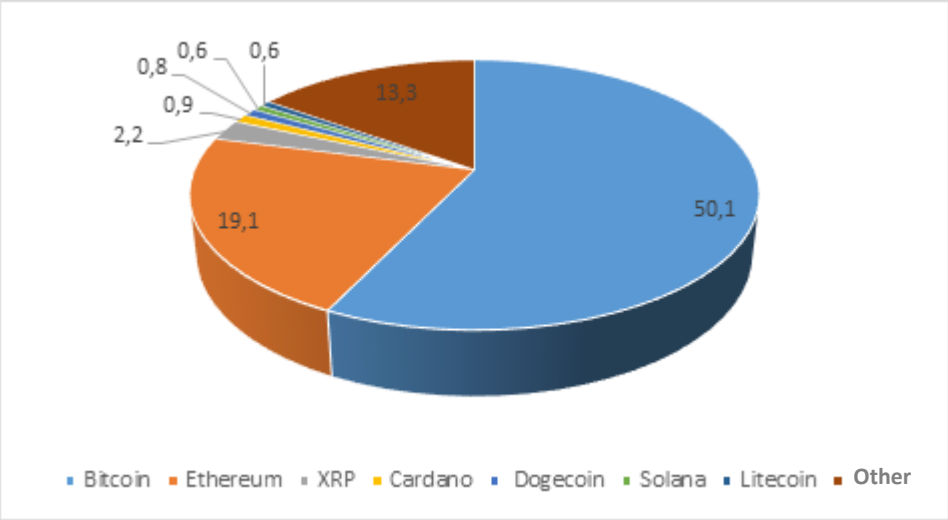
Table 22. Selected types of cryptocurrencies

Type of cryptocurrency	Percentage
Bitcoin	50.1%
Ethereum	19.1%
XRP	2.2%
Cardano	0.9%
Dogecoin	0.8%

[281] https://coinmarketcap.com/
[282] https://coinmarketcap.com/charts/

Solana	0.6%
Litecoin	0.6%
Other	13.3%

Chart 15. Percentage of particular cryptocurrencies in the entire cryptocurrency market (as at 30 June 2023)



628. In accordance with the information available on the website of the Regional Revenue Administration Office in Katowice[283], as at 28 August 2023, the register of virtual currency service providers included 914 entities.

629. In accordance with the information from coinatmradar.com, at least 265 bitcoin ATMs were is use in Poland as at 29 August 2023 (compared to 105 in 2021). Entities operating bitcoin ATM networks are obligated institutions within the meaning of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, and are subject to obligatory entry in the register of virtual currency service providers.

630. The number of bitcoin ATMs in Poland (but also worldwide) is constantly growing. The high rate of the growth in the number of these devices shows that there are more and more people interested in quick exchange of cryptocurrencies, e.g. for cash (despite high commissions on such transactions). According to coinatmradar.com, as at the end of December 2014, there were 301 bitcoin ATMs in the world, while as at 30 June 2023, their number was 35,890.

631. The increasing number of bitcoin ATMs in Poland and around the world also translates into an increase in the number of their manufacturers. According to the data available at coinatmradar.com[284], the main manufacturers of these devices (as at 30 June 2023) worldwide included General Bytes (32.1% market share), Genesis Coin (22.7% market share) and BitAccess (21.5% market share). In Europe, including Poland, the main manufacturers of these devices included General Bytes (62.2% market share), Shitcoins Coin (15.0% market share) and Lamassu (8.5% market share).

[283]https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych
[284] As at 30 June 2023

Chart 16. The largest bitcoin ATM manufacturers worldwide (as at 30 June 2023)

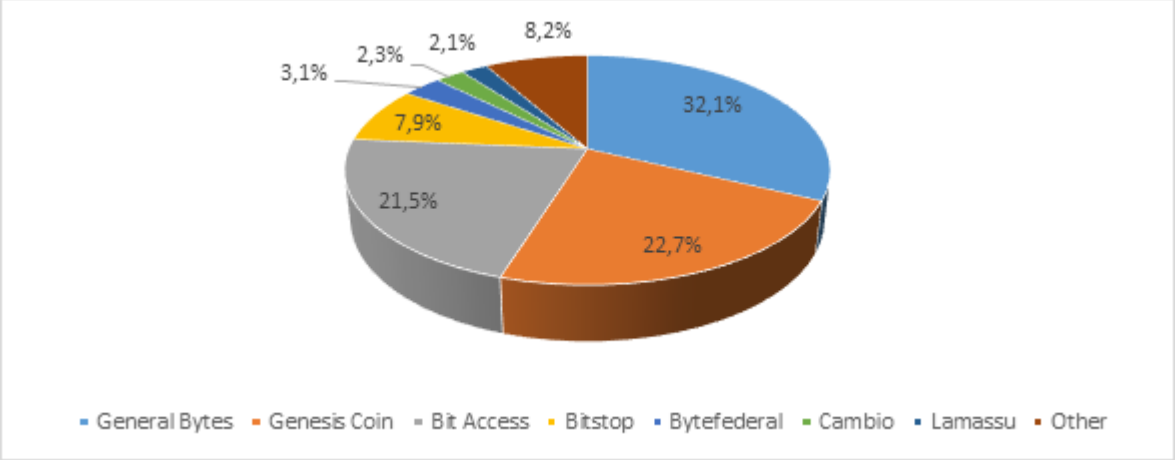
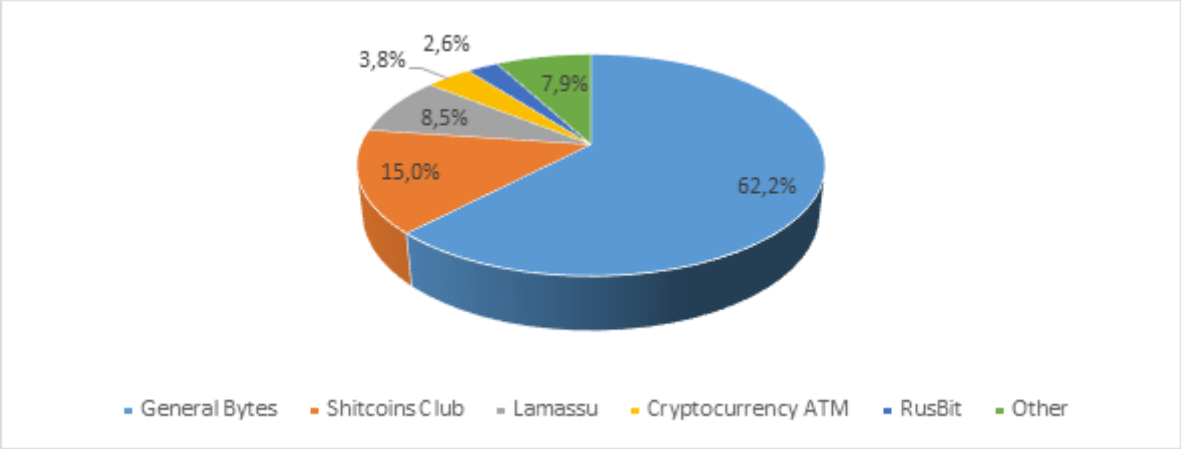


Chart 17. The largest bitcoin ATM manufacturers in Europe (as at 30 June 2023)



632. Cryptocurrency trading services are provided both online and in land-based outlets. Providers of these services enable their customers to buy or sell a certain number of units of decentralised virtual currencies. They do not offer storage services for these units or private keys to access them.

633. Cryptocurrency exchanges offer a wider range of services. Buy and sell transactions involving cryptocurrency units can be concluded with a cryptocurrency exchange, as well as – based on matching buy and sell offers of its customers – between their different users. They also offer their customers management of electronic wallets on their behalf.

634. Unlike legal tenders, decentralised virtual currencies do not have equivalents in the form of banknotes and coins, and are not subject to control exercised by a central bank or other public authorities (lack of supervision and financial guarantee by the state). Moreover, the possibilities of concealing the identity of their users, as well as tools to mix and tumble transactions in order to complicate the connections between them and their users[285] are well developed. This reduces the ability to trace cash flows and verify data concerning their holders.

635. There are two types of payment tokens:

[285] So-called anonymisers, i.e. tumblers, mixers.

- cryptocurrencies that are not issued or guaranteed by the central bank of a given country, and are not money, i.e. a legal tender or fiat currency[286]. These currencies do not meet the criterion of universal acceptability, e.g. in service and commercial outlets. Their value does not depend on the value of another asset (e.g. gold, fiat currency, and is determined based on their popularity among other investors),
- stablecoins. These are tokens whose value is permanently linked to the value of a commodity in circulation, e.g. gold or an official currency. They may, subject to additional requirements provided for in the *Act on payment services*, meet the definition of electronic money.

636. Due to the relatively limited market for trading in payment tokens, holders of a significant amount of cryptocurrency can significantly affect its price. In the case of lesser-known cryptocurrencies, its value can be artificially inflated (e.g. by massively publishing messages on social media containing enthusiastic opinions about a given asset) to attract investors. Then, once the desired level of this value is achieved, the organisers of such a scheme sell their cryptocurrencies (pump and dump mechanism). They make a significant profit, while other investors suffer losses as a result of a significant drop in the price of the cryptocurrency concerned.

637. The analytical proceedings conducted by the GIFI in 2019-2022 included cases relating to suspicions of money laundering using, among others, virtual currencies. They were related to, among others, suspicions of criminal activities involving pyramid schemes or trafficking in psychoactive substances (e.g. drugs).

638. Additional risks related to virtual currencies include the inability of public administration authorities to monitor trade in virtual currencies (in particular cryptocurrencies), as well as the concentration of ownership of some virtual currencies, which facilitates the manipulation of their value.

639. It is worth noting the ease of transferring significant assets in the form of cryptocurrencies in hardware wallets, such as Trezor or Ledger Nano S, that can store an infinite amount of a given cryptocurrency in the form of the so-called "cold wallet". Hardware wallets are physical devices designed to store cryptocurrencies. They contain offline private keys and cannot connect to the Internet or run complex applications, so they are protected against external attacks.

640. In the case of cryptocurrencies, it is worth paying attention to the possible ways of using Distributed Ledger Technology (DLT) to raise funds for various purposes. Initial coin offerings (ICO) are simply another form of obtaining funds for various types of projects, including those related to FinTech.

641. The risk of using ICOs for money laundering or financing of terrorism is related to their following characteristic features:

- lack of transparency in the use of raised funds;

[286] A currency that is not based on material goods (such as bullion), whose value usually comes from a legally decreed monopoly in using it in a given area as a legal tender, and from the demand generated by state institutions.

- cross-border nature of transactions (raising funds from entities from different parts of the world);
- the ease of using straw men or fictitious personal data to legalise assets originating from crime, invested in real projects or ones designed especially for this purpose.

642. It is also worth noting that some public authorities from various countries have issued warnings regarding the risks related to ICOs[287]. In the case of a significant part (approx 30%) of entities in the early stage of development that carried out initial coin offerings (ICO), the market value of the issued crypto-assets dropped to zero, while in the case of the vast majority of them, the values of the entities and the tokens they issued were below the issue price set at the ICO. Based on the available information, it is estimated that in approx. 80% of fundraisers using ICOs, the promised crypto-assets are not actually issued or their issuers "disappear" after they have raised fund from investors.

643. The main problem related to virtual currencies is level of their technological advancement, which currently makes it difficult to analyse transactions, investigate the source of assets and suspend or block a given transaction where money laundering or financing of terrorism is suspected. It should also be noted that due to their features, virtual currencies (mainly cryptocurrencies) may also hinder the application of specific restrictive measures.

644. Current macroeconomic conditions, in particular low interest rates on bank deposits and a dynamic increase in the value of some crypto-assets, make investors look for alternative forms of investing their savings that could potentially bring higher rates of return. In such circumstances, there are entities that offer, often as part of the so-called aggressive marketing (characterised by incomplete or insufficient information to assess risk), the opportunity to invest in broadly understood crypto-assets, including virtual currencies. The security of invested funds requires knowledge and awareness of the risks associated with such forms of investment.

645. It should be noted that the market for cryptocurrencies and crypto-assets (excluding investment tokens that have features similar to financial instruments both in Poland and in other countries) is not governed by specific regulations. Since it is not part of the financial market within the meaning of the *Act of 21 July 2006 on financial market supervision*, it is not supervised by the competent supervisory authorities.

FOREX

646. In accordance with the definition presented by the Polish Financial Supervision Authority, the foreign exchange (Forex) market originally referred to the actual currency exchange market referred to as the interbank market. This market is accessible mainly for banks (hence the term interbank market), as well as to international corporations, governments, central banks and institutional investors. The trading in this market involves currencies and currency derivatives, most often, however, with the delivery of the underlying instrument, which means that actual purchase/sale transactions of specific currencies are carried out in the interbank Forex currency market.

647. Services relating to the Forex market are offered by both domestic and foreign entities. In the case of domestic entities, these are brokerage houses and banks (both banks authorised

[287] Information contained in the warning of the Polish Financial Supervision Authority on the risks related to the purchase of and trading in crypto-assets (including virtual currencies and cryptocurrencies) of 12 January 2021.

to conduct brokerage activities and "ordinary" banks operating under the *Act of 29 August 1997 – Banking Law*).

648. Polish residents also have access to the offers of foreign entities, often via the Internet. In accordance with the relevant legal provisions, such an offer may be provided by foreign investment companies conducting brokerage activities in Poland through a branch or on a cross-border basis – with no need to open a branch, that are established in the territory of the European Union or the European Economic Area and have notified the conduct of such activities or hold the relevant authorisation of the Polish Financial Supervision Authority.

649. Investing in the Forex market involves risk. Investments in derivatives, including contracts for difference (CFD)[288], contain an element of financial leverage, which may result in significant losses that may even exceed the capital held.

650. Investors trading in the FOREX market hope to make a profit on increases in the rates of currencies, raw materials, shares or commodities, or on their decreases. However, these transactions are largely speculative because "... the Forex market is difficult to predict for an individual and inexperienced investor, especially where the other party to the transaction is a Forex broker who controls all the data on its trading platform and has information on the orders of all its clients"[289].

651. The FOREX market and transactions concluded on it may be used to commit predicate offences for money laundering. This may involve fraud based on misleading customers[290] (e.g. by providing false expert opinions or financial analyses) or favouring certain customers (e.g. by providing them with confidential information about the orders of other customers), computer offences (e.g. related to unauthorised access to customer accounts) as well as offences involving corruption.

652. As in the case of other financial institutions, it is also possible to use the FOREX market for money laundering, in particular where the broker is controlled by criminals and orders are placed by criminals or individuals representing them.

Securities

653. In accordance with Article 3(1) of the *Act of 29 July 2005 on trading in financial instruments*, securities mean:

(a) shares, pre-emptive rights within the meaning of the *Act of 15 September 2000 – Code of Commercial Partnerships and Companies* (Journal of Laws of 2022, item 1467), rights to shares, subscription warrants, depository receipts, bonds, mortgage bonds, investment certificates and other transferable securities, including those incorporating

[288] A CFD is an agreement between a "buyer" and a "seller" to exchange the difference between the current price of the underlying instrument (e.g. shares, currencies, commodities, indices, etc.) and the price of the instrument at the close of the contract. CFDs are leveraged products.

[289] Maciej Kurzajewski i Dorota Nowalinska, Zysk a ryzyko na rynku FOREX. Poradnik klienta usług finansowych, KNF, Warsaw, 2017, p. 22 (at: https://www.knf.gov.pl/knf/pl/komponenty/img/Zysk%20a%20ryzyko%20na%20rynku%20Forex_59289.pdf).

[290] Cf.: 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/

property rights corresponding to rights arising from shares or debt assumption, issued under relevant provisions of Polish or foreign law;

(b) other negotiable property rights that arise from an issue, incorporating the right to purchase 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, rates of return, commodities and other indicators or measures (derivative rights).

654. Securities may be traded as part of organised trading or over-the-counter.

655. Although Chart 12 *(Completed analytical proceedings initiated by the GIFI in 2020-2022, broken down by products and services used for suspicious transactions)* shows that only a small part of the analytical proceedings initiated and carried out by the GIFI 2020 – 2022 2022 concerned capital market instruments (i.e. not only securities, but also other financial instruments, including derivatives), this does not mean that the risk of their use for money laundering is small. In particular, attention should be paid to the possibility of trading shares outside the public market.

656. ML/FT risks relating to securities markets are identified in the following methods of money laundering and financing terrorism. The basic method of money laundering using securities involves cash deposits into a cash account followed by withdrawals, also in cash. The document collected upon withdrawal confirms that the money comes from an account used to handle securities transactions. Other ML/FT methods include: crediting and debiting the cash account with cashless transactions not related to trading in securities, crediting the cash account combined with the purchase and sale of securities, transferring securities, and crediting the cash account with funds from a loan.

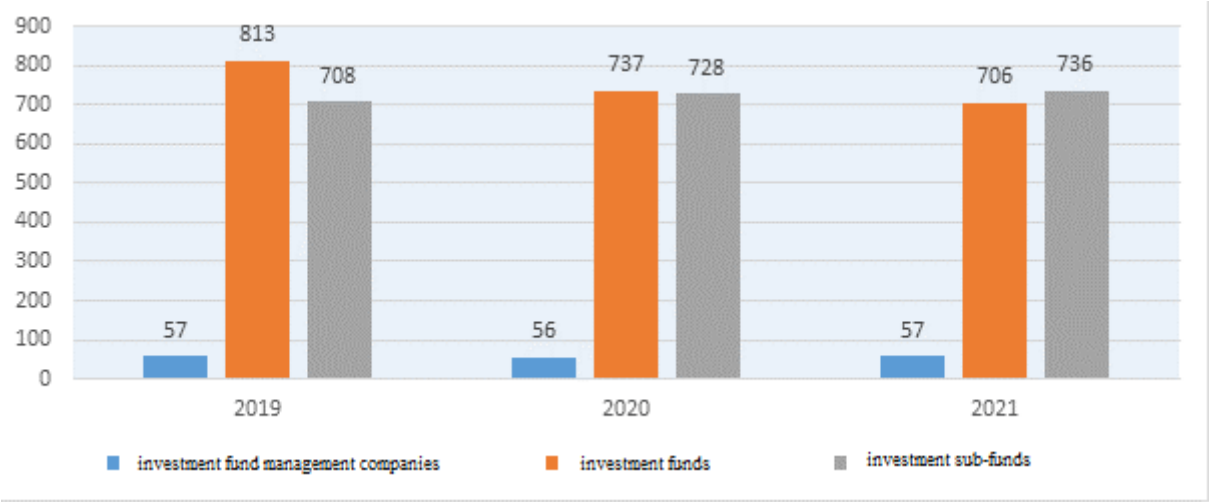
Investment funds

657. According to the information contained in the Polish Financial Supervision Authority's report for 2021, 57 investment fund management companies were authorised to operate in Poland, managing a total of 706 investment funds, including: 45 open-end investment funds, 69 specialist open-end investment funds, and 592 closed-end investment funds.

658. Figures regarding particular investment funds, investment fund management companies and sub-funds in 2019 – 2021 are presented in the chart below.

Chart 18. The total number of supervised investment fund management companies, investment funds and sub-funds in 2019-2021[291]

[291] Data of the Polish Financial Supervision Authority for 2021



659. Risks related to the operation of investment funds usually refer to broadly understood investment risk. The Polish Financial Supervision Authority defines it as "uncertainty as to the final outcome of the investment". For this reason, an investment fund, both open- and closed-end, never guarantees that the investment objective indicated in the fund's statute will be achieved. The source of risk may be various macro- and microeconomic factors that directly or indirectly affect the market valuation of the fund's assets"[292].

660. According to the report prepared by the Chamber of Fund and Asset Managers[293], in 2020, the capital market was affected to the greatest extent by the COVID-19 pandemic that resulted in high volatility in this market. According to the data contained in the aforementioned report, in 2020, stock indices were subject to significant fluctuations caused by the incoming information about the course of the pandemic, as well as steps taken by central banks and governments of particular countries.

661. When considering the operation of investment funds in terms of the risk of their use for money laundering, it should be noted, first of all, that perpetrators may invest proceeds from crime in investment funds just like in other financial services. This may take place as part of a broader plan for the use of various products and services offered in the financial market, providing for the use of purchase and immediate sale transactions involving participation units or investment certificates as one of the intermediate stages of money laundering. Investment funds may also be the ultimate destination for laundered funds. In both situations, and especially in the latter, it will probably be important for the perpetrators to assess the investment risk and the possible loss of the entrusted funds.

662. When considering ML/FT risk, particular attention should be paid to closed-end investment funds due to their characteristic features that may facilitate these offences. First of all, unlike open-end investment funds, their offer is usually addressed to a narrower group of participants.

[292] Agnieszka Siwek, Łukasz Wojakowski, Jednostki uczestnictwa i certyfikaty inwestycyjne funduszy inwestycyjnych – porównanie zagadnień prawnych i organizacyjnych. Poradnik klienta usług finansowych, KNF, Warsaw, 2016, p. 11, at: https://www.knf.gov.pl/?articleId=54141&p_id=18.
[293] Raport roczny IZFiA za rok 2020 (Annual report of the Chamber of Fund and Asset Managers for 2020), p. 33

663. Some assessments of the activities of closed-end investment funds indicate that they create favourable conditions for tax optimisation and money laundering[294]. ML risk in the case of closed-end investment funds is due primarily to their following features: collecting and investing funds from a closed group of natural persons and business entities, wider investment opportunities than in the case of other types of investment funds, and opportunities to invest in various assets, both domestic and foreign ones.

Telecommunications services linked with mobile payments

664. There are different definitions of what can be considered a mobile payment. According to the Central European Bank it is a financial transaction where a mobile device is used at least to initiate a payment[295]. In this case, a portable device designed to connect to services or websites using radio technology or telecommunications networks using radio technology is used. Such a device must also have a keyboard or other type of interface intended for communication with the user and sufficient space for storing information used to confirm the user's identity.

665. Mobile payments enable the direct purchase of goods or services and the transfer of funds between the bank accounts of the buyer and the seller. Payments are divided according to the way the mobile device communicates with the data processing centre, i.e. into:

(1) remote mobile payments as the most popular type of mobile payments. This involves a connection between a mobile phone and a server via a text message (the so-called Premium SMS) or the Internet. Premium SMS is most often used as a form of payment for press articles available online, participation in competitions, voting in TV shows or online access to videos. The buyer enters in a text message the code indicated by the seller and sends it to the indicated number. In response, the buyer receives a reply message confirming the sending of the text message or a code that can be entered on the website to enable access to the content they are looking for.

(2) Contactless mobile payments enabled by the Near Field Communications (NFC) technology. This wireless technology relies on the use of radio waves to exchange data over a short distance, usually a few centimetres. Payment cards based on the NFC technology are brought close to the device enabling authorisation, thanks to which a connection is established and data transfer takes place (an exchange of messages resulting in the transfer of funds). The NFC technology also works in mobile phones, that thus become mobile wallets. They work on the same principles as payment cards, i.e. the payer has to bring the phone close to the terminal to make a payment. There are many applications in the market that use this technology. It is offered in commercial bank applications, as well as by Revolut, PayPal, etc. With such an application, the user can make payments by holding the phone close to the payment terminal.

666. During the COVID-19 pandemic, an increase in mobile payments was recorded. According to *Płatności Cyfrowe 2020* (Digital Payments 2020) report, in 2020, at least 27% of

[294] Some information shows that there are difficulties in determining the beneficial owners of such funds due to the refusal to provide information about participants of these funds to other obligated institutions intermediating in transactions carried out as part of these funds.
[295] All glossary entries (europa.eu), access on 07.06.2022

respondents declared that they intended to make electronic purchases more often due to the coronavirus epidemic. In April – June 2020, there was a 10% increase in the amount of purchases paid for through contactless transactions[296]. According to PRNews.pl, in the first quarter of 2022, there were 8,305,957 HCE cards registered in Poland, that were used for contactless payments via mobile phones[297], which represents an increase by 933,096 quarter-on-quarter and 1,809,923 year-on-year. This process was accelerated after the contactless payment limit was increased from PLN 50 to PLN 100 in 2020. This change also covered contactless payments made via mobile devices.

667. In the aforementioned report, it was indicated that BLIK and mechanisms based on HCE cards were the fourth most commonly used transaction product indicated by the respondents. The number of transactions made in this way is constantly growing. In the first quarter of 2022, 247 million transactions with a total value of PLN 32.6 billion were made using BLIK alone, which is an 63% increase year-on-year. The substantial part of these payments related to online purchases – 156.3 million transactions with a total value of PLN 18.8 billion. BLIK was also used to make phone transfers – 44.1 million transactions worth PLN 5.1 billion, payments at payment terminals and ATM withdrawals – 8.6 million and 10.2 million transactions, respectively[298].

668. The BLIK payment system is now undoubtedly the most popular mobile payment system unrelated to a physical medium. BLIK is classified as a payment system supervised by the National Bank of Poland[299]. BLIK allows for making payments using portable devices (e.g. mobile phones and tablets), both online and in traditional stores and commercial outlets, in public transport, public offices, and between users (P2P). At the end of 2015, the Polish Payment Standard introduced the peer-to-peer (P2P) service, i.e. mobile payments between mobile phone users, as part of the BLIK system. The service allows its users to instantly transfer money to another person without having to provide this person's bank account number, but only by entering their phone number. All the BLIK system user has to do to enable this service is to link its telephone number with its bank account number in the application. Transactions using a portable device have been possible since 9 February 2015. To use the available services, the user has to download the mobile application of one of the BLIK system participants. The development of this method has led to an increase in the number of offences related to deceitfully obtaining funds using this mechanism, most often by impersonating a person using BLIK and asking friends or random people to provide a code. The code is often used to withdraw cash from an ATM[300] or buy cryptocurrencies. In this case, criminals often use highly developed attack methods, most often phishing and advanced social engineering[301]. The main problem is that a transaction, e.g. withdrawing cash from an ATM using a BLIK code, can be made instantly. Fraud in this payment system can also be used to commit a more complex

[296] Płatności Cyfrowe 2020 (Digital Payments 2020)
[297] Report posted at PRNews.pl: Liczba mobilnych kart zbliżeniowych Google Pay, Apple Pay i HCE – I kw. 2022 - PRNews.pl, access: 01.06.2022
[298] BLIK: mocny początek roku – blisko ćwierć miliarda transakcji i 10,5 mln aktywnych użytkowników w pierwszym kwartale 2022 r. | BLIK, access on: 02.06.2022
[299] List of systems supervised by the President of the National Bank of Poland
[300] Jak przestępcy wykorzystują BLIK? - legalniewsieci.pl, access on 03.06.2022
[301] » Ojciec oszukał mnie przez Facebooka. Czyli dwa ataki świetnie przygotowanego złodzieja z kryptowalutami w tle -- Niebezpiecznik.pl -- access on: 03.06.2022

offence[302]. In this case, there is no need to wait for funds to be transferred between banks or accounts in a given banking institution. The ability to use the code instantly to collect money makes it possible to transfer it to people who may use it for illegal purposes. It should be noted that any person, even an anonymous one, can collect cash using a BLIK code. There is a risk that payments made in this way may be used to transfer illicit funds using a network of "mules" moving money within a network of extensive transactions. Registration data of legally operating companies may also be used in such mechanisms. Those participating in this illegal practice may even be unaware that they are involved in money laundering[303]. EUROPOL informed about recruiting unaware people for moving and laundering money after the completion of the EMMA4 operation in 2018[304].

669. Transactions made using mobile devices make it possible to make payments using funds deposited in the account in cash. The account can be topped up through a regular transfer using, among others, PayPal. This enables introducing cash into circulation that can later be used, among others, by making mobile payments. The account can be topped up with cash, e.g. using the services of Poczta Polska S.A.[305], or by any other type of remittance, also from an anonymous person.

670. Another issue is the possibility of transferring funds using devices dedicated to fundraisers using mobile payments[306,307]. Such devices make it possible for various people to freely access them and deposit money. This risk is combined with other risks, such as the possible abuse of foundations and social associations for money laundering or financing of terrorism, the use of prepaid cards, etc. Control over the depositing process is limited to the transfer of funds between accounts. The moment of making a payment is not supervised as devices are located in publicly accessible places, including shopping centres, places of worship, etc., which makes it possible to make a payment by unidentifiable persons, as long as they use false data.

671. The threats related to new mobile payment media such as implants[308] and NFC gadgets[309] are yet unknown. They allow for the secret transfer of monetary values in electronic form. Paired with an account in the mobile payment system, it can be easily used to finance various activities in the country where a given form of payment is accepted. While this payment method is not very popular in Poland, its use by people of foreign origin is possible.

Gambling

672. The operation of the gambling market in Poland is regulated by the *Gambling Act of 19 November 2009* and the implementing regulations thereto. In accordance with the aforementioned Act, gambling games include games of chance, betting, card games and games

[302] Mieszkaniec powiatu krakowskiego stracił aż 130 000 zł. Oszustwo z wykorzystaniem BLIKa. Jak to w ogóle możliwe!? (sekurak.pl), access on 03.06.2022
[303] Facebook, BLIK, Gadu-Gadu, BitBay i stado nieświadomych mułów | Zaufana Trzecia Strona, access on: 03.06.2022
[304] Over 1500 money mules identified in worldwide money laundering sting | Europol (europa.eu), access on: 03.06.2022
[305] https://pomoc.home.pl/baza-wiedzy/jak-doladowac-konto-paypal#1, access on: 07.06.2022
[306] Bezgotówkowa ofiara na kościół (liturgiczny.pl); access on: 03.06.2022
[307] Zbiórkomat - Innowacyjne Rozwiązania - DlaFundacji, access on: 03.06.2022
[308] https://gomobi.pl/blogi/wszczepilem-w-reke-implant-platniczy-to-moje-pierwsze-wrazenia/, access on: 07.06.2022
[309] https://www.telepolis.pl/fintech/cashless/nfc-evering-pierscien-platnosci-zblizeniowe, access on: 07.06.2022

on gaming machines. Games of chance are games, including those arranged online, where the prize is either of a pecuniary or material nature, and whose result is primarily determined by chance. These are: draw-based games, lotteries, telebingo, cylindrical games, dice games, cash bingo games, raffle bingo games, raffle lotteries, promotional lotteries, and audio-text lotteries. Betting involves bets for pecuniary or material prizes, consisting in guessing the results of a sports competition between people or animals, in which participants pay stakes, and the amount of the prize depends on the total amount of the paid stakes (sweepstakes), as well as guessing the occurrence of various events, including virtual ones, in which participants pay stakes, and the amount won depends on the ratio of the payment to the prize agreed between the host bet and the payer (bookmaking). Games on gaming machines are games of chance that are played with the use of mechanical, electromechanical or electronic devices, including computer hardware, and games with rules corresponding to the rules of games on gaming machines arranged online, where the prizes are of a pecuniary or material nature, and where the game contains an element of chance. Card games include black jack, poker and baccarat, if played for pecuniary or material prizes.

673. The aforementioned *Gambling Act* introduced a state monopoly in the organisation of gambling. Since then, only licenced entities have been allowed to arrange gambling games. The information on the implementation of the *Gambling Act* in 2020 includes the following data regarding legal gambling (table below)[310]:

Table 23. Data regarding the gambling market in 2019-2021

Item	Number of valid authorisations/licences			Number of gaming facilities covered by granted licences/authorisations			Number of issued authorisations/licences		
	2019	2020	2021	2019	2020	2021	2019	2020	2021
Casinos	51	51	50	51	51	50	6	1	1
Cash bingo arcades	0	0	0	0	0	0	0	0	0
Betting shops (bookmaking and sweepstakes)	30	31	27	2,423	2,210	1,888	4	5	3
Online betting	18	19	23	X	X	X	5	2	6

674. The gambling market is controlled by the National Revenue Administration. The tasks of the National Revenue Administration (KAS) include customs and tax controls in the area of gambling games as well as recognising, detecting, preventing and combating fiscal crimes and fiscal offences against the organisation of gambling games and prosecuting their perpetrators, as well as tax controls regarding gaming tax and fees. As at the end of 2020, a total of PLN 34,329,900.00 was transferred to the state budget on account of all fees related to the organisation of gambling games (licence issuance fees, device registration fees, etc.). At the same time, information was provided on the amount of arrears covered by writs of execution as at 31 December 2020, in the amount of PLN 4,646,000.00, of which tax arrears of PLN 115,600.00 were recovered.

675. The amendment to the *Gambling Act* in 2016 introduced a strict state monopoly on games on gaming machines outside casinos and arranging gambling games on the Internet. Due

[310] Information on the implementation of the Gambling Act in 2020

to the broad definition of gambling and very strict market control some of the activities of gambling companies have been moved to the Internet. These activities are very often carried out from servers located outside Polish jurisdiction. Since 1 April 2017, a register of websites offering illegal online gambling has been maintained by a specialised unit of the Opole National Revenue Administration. Since 1 July 2017, communications service providers have been obliged to block domains listed in the register. Total Casino owned by Totalizator Sportowy[311] is the only legal online casino. Based on H2 Gambling Capital data, the Ministry of Finance reported that the revenue of the gambling sector in Poland increased in 2021 by 52.5% (i.e. PLN 14.18 billion) compared to 2020. It was also indicated that the underground online gambling market is decreasing year by year (see: table below[312]):

Table 24. Data regarding the underground gambling market in 2016-2021[313]

Item	2016	2017	2018	2019	2020	2021
Total underground gambling market in Poland	79,70%	44,40%	34,70%	25,40%	22,80%	17,90%
EU average of the total underground gambling market*	44,00%	38,80%	35,30%	30,00%	27,40%	25,20%
Underground betting in Poland	64.30%	20.30%	13.50%	10.30%	9.40%	8.20%
EU average of underground betting	41.20%	36.00%	33.20%	29.60%	27.90%	27.90%
Underground casino games in Poland	100.00%	100.00%	98.80%	68.90%	54.00%	37.70%
EU average of underground casino games	69.90%	61.10%	58.20%	48.70%	44.60%	40.00%

676. Entities whose illegal services are offered on the Polish market also take steps to avoid blocking their activities[314], consisting most often in cloning the addresses of websites

[311] Total Casino – Wikipedia, wolna encyklopedia, access on: 14.06.2022

[312] Sytuacja na rynku gier hazardowych *on-line* - Ministerstwo Finansów (Situation on the online gambling market – Ministry of Finance) – gov.pl (www.gov.pl), access on: 14.06.2022

[313] Slightly different data is presented in the report of the consulting company EY, prepared in cooperation with the Graj Legalnie association. The research institution estimated that in Poland, in 2016-2020, the turnover generated by the illegal part of the online gambling market increased from PLN 3.5 billion to PLN 12.6 billion, which translated into losses for the state budget of over PLN 2 billion. In 2020, shadow economy turnover accounted for 46.7% of the online gambling market. Taking net revenue as the determinant, the value of underground online gambling was estimated at PLN 1.1 billion, i.e. 34.5% of the net revenue of the entire market {data from the Graj Legalnie website: For underground online gambling to be limited, education is crucial – Hazard News, access on: 14.06.2022}

[314] It is also noted that approx. 15.5% of Internet users in Poland admit to using illegal online gambling. Approximately 2.7 million people use online casinos, that – in accordance with the Gambling Act – are illegal, while 1.4 million people place bets with bookmakers that do not pay taxes in Poland. Some users (approx. 16%) use VPN systems to bypass the block or use foreign and virtual currencies (approx. 22%) {information from the article: "Tak Polacy obchodzą ustawę hazardową. Państwo przymyka na nich oko" (This is how Poles circumvent the gambling law. The state turns a blind eye to them) – Money.pl, access on: 14.06.2020.

containing minor changes to those included in the register[315]. The aforementioned H2 Gambling Capital report shows that Poland is doing well in blocking illegal services.

677. The Gambling market in Poland report prepared by the Association of Private Employers in December 2021 indicated that the most serious determinants of the development of underground gambling include, among others, insufficient control mechanisms, fiscal burdens prompting game operators to offer their services illegally and customers to use such services, dynamic technological development offering new ways of doing business, some users' ignorance about applicable regulations, inconsistency and defective creation of regulations allowing for taking advantage of loopholes in the law. Moreover, the use of the illegal online gambling offer increased in 2020-2021 due to the COVID-19 epidemic[316]. The pandemic also caused a delay in the construction of a legal network of amusements arcades run by Totalizator Sportowy[317]. Illegal arcades did not respect lockdown regulations.

678. The problem of illegal gaming halls with gaming machines remain unsolved. Well-organised illegal enterprises, often located in illegal venues and operated by employed foreigners bring significant profits[318]. In 2020, the National Revenue Administration reported that since 2017, it had seized approx. 50,000 illegal gaming machines[319]. Single groups involved in organising illegal games on gaming machines can have a significant reach. For example, in November 2021, the National Revenue Administration reported the dismantling of a criminal group having at its disposal 30,000 gaming machines, installed in over 9,700 location throughout Poland[320]. It should be noted that illegal gambling is often accompanied by money laundering, as in the case described by the National Revenue Administration in 2021, where 37 persons suspected of organising illegal games on gaming machines were detained in 2018-2021. The illegally obtained income was used to purchase real estate and movable property through straw men, family members and business entities controlled by criminals. In addition, the suspects used bank accounts outside Poland to withdraw funds from them in cash. This money was then used to finance mortgage loans. Those involved earned from their activities over PLN 50,000,000.00[321].

679. Illegal game arcades also make technological changes in their operations. Mechanical gaming machines are being replaced with workstations containing virtual gaming software. Such devices make it difficult to prove that they have been used for gambling[322] and make it possible to disguise an arcade as an internet cafe[323]. It is also indicated that in some arcades

[315] Nielegalny hazard kwitnie pomimo zmian w prawie. Raport NIK rozwiewa złudzenia (Illegal gambling thrives despite changes in the law. The Supreme Audit Office's report dispels illusions) (spidersweb.pl), access on 14.06.2022.
[316] Rynek hazardowy w Polsce, ZPP, grudzień 2021
[317] Totalizator Sportowy: do końca czerwca ma ruszyć 700. salon gier na automatach - Bankier.pl, access on: 17.06.2022
[318] Piwo, dym i żadnych pytań. Tak działają nielegalne kasyna - Money.pl, access on; 17.06.2022
[319] Walka z jednorękimi wiatrakami - Bankier.pl, access on: 17.06.2022
[320] https://www.gov.pl/web/kas/kas-rozbila-grupe-nielegalny-hazard; access on: 17.06.2022
[321]https://www.gov.pl/web/prokuratura-krajowa/zatrzymani-za-nielegalny-hazard-oraz-pranie-brudnych-pieniedzy, access on: 17.06.2022
[322] Totalizator Sportowy: do końca czerwca ma ruszyć 700. salon gier na automatach - Bankier.pl, access on: 17.06.2022
[323] To nie była kawiarenka internetowa, ale salon gier hazardowych (24kurier.pl), access on: 17.06.2022

ATMs/cash deposit machines are installed, allowing for unattended operation[324]. There are regular reports of the use of force against National Revenue Administration officers carrying out inspections, in particular securing arcades using as sophisticated devices as remote activated pepper spray and other lacrimator dispensers[325].

680. As a rule, gambling is associated with possible money laundering. There are many opportunities to make payments in this way, e.g. intentionally losing money by one player to another, using an account associated with gambling to receive alleged winnings, etc.[326]. In the past, it also happened that money was laundered as part of official gambling, e.g. publicly organised, completely legal lotteries. The mechanism involved criminals buying winning tickets with illegally obtained money and collecting legal winnings[327]. The Polish press also reported on criminals attempts to contact lottery winners[328].

7.2.2. Vulnerability of the non-financial market

681. The online surveys that the GIFI sent to obligated institutions and cooperating units[329] in August 2021 included a request to indicate (maximum) 5 products and services offered outside the financial market that are or can be most often used for money laundering. Obliged institutions and cooperating units selected responses from a list containing the following items:

- telecommunications services involving premium rate numbers (Premium services),
- cryptocurrencies,
- quick digital transfer orders (e.g. TransferGo),
- centralised convertible currencies used for asset transfers (e.g. Webmoney, Perfectmoney),
- physical cross-border transportation of assets by natural persons,
- cargo services, courier and postal parcels,
- buying/selling casino chips,
- games on gaming machines,
- games of chance (other),
- poker and other similar games,
- betting,
- online gambling games,
- crowdfunding,
- services provided by lawyers, legal counsels,

[324] Nalot na nielegalny salon gier w Świeciu. Po raz drugi w tym samym miejscu | Extra Świecie (extraswiecie.pl), access on: 17.06.2022
[325] Gazem pieprzowym w kontrolera - na taki pomysł wpadli w bezobsługowym "salonie gier". Czy takie zabezpieczenia są legalne? (bezprawnik.pl), access on: 17.06.2022
[326] *On-line* gambling as a money laundering method - AMLC.EU, access on: 17.06.2022
[327] Mafiosi prali pieniądze na loterii - Dziennik.pl, access on: 17.06.2022
[328] Wygrana w Lotto haracz: fakty i mity - Pomoc Po Wygranej, access on; 17.06.2022
[329] For more information go to Chapter 7.2.1.

- services provided by notaries,
- services provided by expert auditors and tax advisors,
- accounting 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 with their registered offices in tax or financial havens,
- trusts,
- companies that do not conduct actual business activities (shell companies),
- services in the field of establishing business entities and trusts and providing services thereto,
- other non-financial products and services.

682. In the case of obligated institutions, 619 responses were received. The total number of responses by the obligated institution category is presented in the table below.

Table 25. Number of survey responses by the obligated institution category

Oligated institutions [330]	Number of survey reponses	
	Number of responses	Percentage

[330] 11 – currency exchange operators, 1 – domestic banks, branches of foreign banks, branches of credit institutions, financial institutions having their registered office in the territory of the Republic of Poland and branches of financial institutions not having their registered office in the territory of the Republic of Poland, within the meaning of the *Act of 29 August 1997 – Banking Law*, 13 – notaries in so far as they perform activities in the form of a notarial deed, 7 – investment funds, alternative investment companies, investment fund management companies, AIC managers, branches of management companies and branches of EU managers located in the territory of the Republic of Poland, within the meaning of *Act of 27 May 2004 on investment funds and alternative investment fund management*, 4 – investment companies, custodian banks within the meaning of the Act of 29 July 2005 on trading in financial instruments and branches of foreign investment companies within the meaning of this Act, conducting business in the territory of the Republic of Poland, 3 – domestic payment institutions, domestic electronic money institutions, branches of EU payment institutions, branches of EU and foreign electronic money institutions, small payment institutions, payment service offices and acquirers, within the meaning of the Act of 19 August 2011 on payment services, 27 – economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, conducting business activities consisting in: trade in or brokerage in the trade in works of art, collectibles and antiques within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services*, also where such activities are carried out: in art galleries or auction houses or using a free port, understood as a zone or room where goods are treated as not located within the customs territories of Member States or third countries, also with the use of a duty-free zone, storage of works of art, collectibles and antiques within the meaning of Article 120(1)(1)-(3) of the *Act of 11 March 2004 on tax on goods and services*, where such activities are carried out using a free port referred to in point (a) second indent- with respect to transactions with a

11	294	47.50%
1	227	36.67%
13	54	8.72%
7	15	2.42%
4	6	0.97%
3	5	0.81%
27	5	0.81%
2	3	0.48%
22	2	0.32%
8	2	0.32%
14	2	0.32%
21	1	0.16%
12	1	0.16%
18	1	0.16%
16	1	0.16%
Total	**619**	**100.00%**

683. According to the aforementioned information, the majority, i.e. 47.50% of the survey responses were submitted by currency exchange office operators (11) and 36.67% by domestic 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 that are not established in the territory of the Republic of Poland, within the meaning of the *Act of 29 August 1997 – Banking Law* (1).

Table 26. Products and services offered outside the financial market – obligated institutions

Products and services offered outside the financial market – obligated institutions	Percentage
games on gaming machines	13.54%
cryptocurrencies	13.11%
activities of non-profit entities (foundations, associations)	13.11%
online gambling games	7.88%
physical cross-border transportation of assets by natural persons	7.02%
business entities with their registered offices in tax or financial havens	5.73%

value equal to or exceeding the equivalent of EUR 10,000, regardless of whether the transaction is carried out as a single operation or several operations that appear to be related to each other, 2 – cooperative savings and credit unions and the National Association of Cooperative Savings and Credit Unions, 22 – entities conducting business activities in the field of games of chance, betting, card games and games on gaming machines within the meaning of the Act of 19 November 2009 on gambling, 8 – insurance companies conducting the activities referred to in Section I of the Annex to the Act of 11 September 2015 on insurance and reinsurance activities, including domestic insurance companies, main branches of foreign insurance companies with an registered office in a country that is not a Member State and branches of foreign insurance companies with a registered office in a Member State other than the Republic of Poland, 14 – notaries with respect to the activities referred to in Article 79(6a)of the *Act of 14 February 1991 – Law on Notaries*, 21 – postal operators, 12 – entities conducting business activities consisting in the provision of services involving: exchange between virtual currencies and legal tenders, exchange between virtual currencies, 18 – economic operators within the meaning of the *Act of 6 March 2018 – Economic Operators' Law*, that are not other obligated institutions (Article 2(1)(16) of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism), 16 – tax advisors with respect to tax advisory activities other than those listed in Article 2(14) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, and expert auditors.

trade in antiques and works of art	5.59%
games of chance (other)	4.94%
purchase/sale of real estate	3.65%
purchase/sale of precious stones and metals	3.44%
companies that do not conduct actual business activities (shell companies)	3.44%
trade in other high-value goods, e.g. cars, boats	3.30%
crowdfunding	3.15%
buying/selling casino chips	2.72%
import/export of goods and services	2.51%
poker and other similar games	2.08%
donation agreements	0.93%
cargo services, courier and postal parcels	0.72%
other non-financial products and services	0.64%
quick digital transfer orders (e.g. TransferGo)	0.57%
betting	0.43%
telecommunications services involving premium rate numbers (Premium services)	0.36%
centralised convertible currencies used for asset transfers (e.g. Webmoney, Perfectmoney)	0.36%
trusts	0.29%
services in the field of establishing business entities and trusts and providing services thereto	0.21%
accounting services	0.14%
services provided by lawyers, legal counsels	0.07%
services provided by notaries	0.07%

The five most frequently mentioned items from the list of products and services offered outside the financial market included: games on gaming machines, cryptocurrencies, activities of non-profit entities (foundations, associations), online gambling, and physical cross-border transportation of assets by natural persons. 'Games on gaming machines' accounted for the greatest percentage of the responses provided by obligated institutions,

684. Online surveys were completed by 202 cooperating units, including government administration bodies, local government bodies and other state organisational units. Particular responses from cooperating units relating to products and services offered outside the financial market are presented in the table below:

Table 27. Products and services offered outside the financial market – cooperating units

Products and services offered outside the financial market – cooperating units	Percentage
cryptocurrencies	9.09%
trade in antiques and works of art	7.27%
business entities with their registered offices in tax or financial havens	7.27%
online gambling games	6.36%
purchase/sale of real estate	6.36%
games on gaming machines	6.36%
companies that do not conduct actual business activities (shell companies)	6.36%
purchase/sale of precious stones and metals	6.36%
trade in other high-value goods, e.g. cars, boats	5.45%
games of chance (other)	4.55%

activities of non-profit entities (foundations, associations)	4.55%
physical cross-border transportation of assets by natural persons	4.55%
cowdfunding	4.55%
buying/selling casino chips	2.73%
import/export of goods and services	2.73%
other non-financial products and services	2.73%
quick digital transfer orders (e.g. TransferGo)	2.73%
telecommunications services involving premium rate numbers (Premium services)	1.82%
poker and other similar games	1.82%
betting	1.82%
cargo services, courier and postal parcels	0.91%
services in the field of establishing business entities and trusts and providing services thereto	0.91%
centralised convertible currencies used for asset transfers (e.g. Webmoney, Perfectmoney)	0.91%
donation agreements	0.91%
trusts	0.91%

Summing up, five products and services offered outside the financial market that were most frequently mentioned by cooperating units included: cryptocurrencies, trade in antiques and works of art, businesses registered in tax or financial havens, online gambling, and purchase/sale of real estate. Cryptocurrencies accounted for the greatest percentage (9.09%) of the five products and services offered outside the financial market that were most frequently mentioned by cooperating units.

685. The survey responses from both obligated institutions and cooperating units were selected from a list of products/services that, as part of the analyses conducted by the GIFI, were often indicated as the *modus operandi* of financial transactions used for money laundering outside the financial market. A wide range/list of possible responses indicated by particular entities participating in the survey allows for identifying specific areas of threats in this respect. The graphical distribution of the five products and services concerned by the respondent type is presented in Chart 19 and Chart 20 below.

Chart 19. Products and services offered outside the financial market – obligated institutions

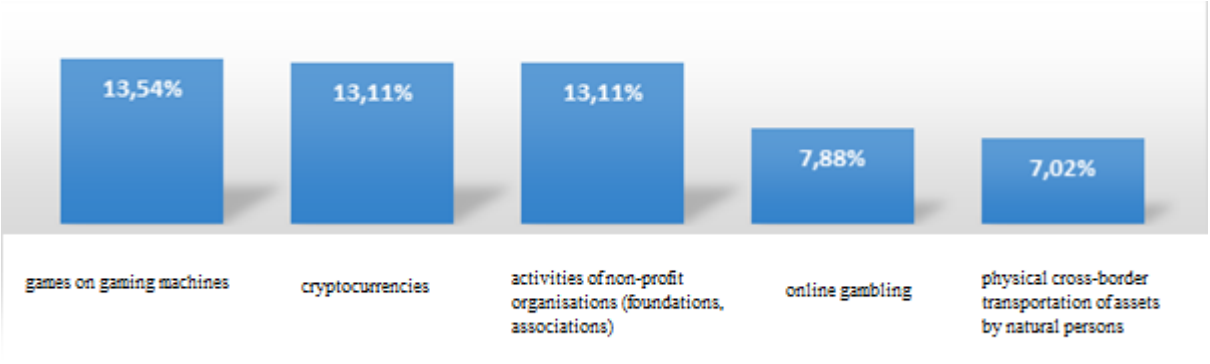
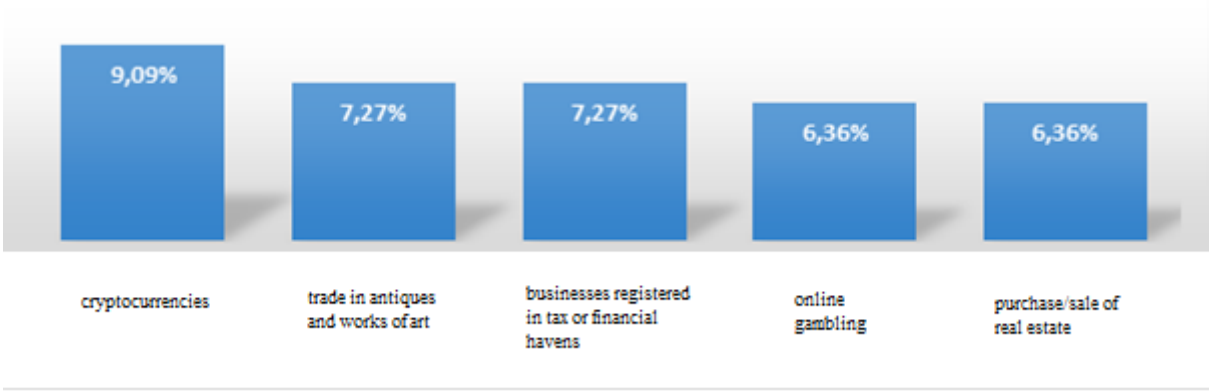


Chart 20. Products and services offered outside the financial market – cooperating units



Summing up, obligated institutions and cooperating entities indicated in their responses the same two products and services offered outside the financial market that were most often used for money laundering. These were cryptocurrencies (number 1 in the survey responses from cooperating units) and online gambling (number 4). At this point, it should also be noted that games on gaming machines (number 1 – Chart 19) were another area at the highest risk of money laundering indicated by the responding obligated institutions. The threats related to these areas, i.e. products and services offered outside the financial market, are described below.

The areas related to cryptocurrencies, games on gaming machines and online gambling have been described previously in Chapter 7.2.1.

Activities of non-profit organisations

686. Recognising non-profit activities as an area of risk of abuse for the purposes of money laundering or terrorism financing is related to the FATF Recommendations. In its Recommendation 8, the FATF indicated that countries should make every effort to ensure that non-profit organisations (NPOs) are not used for money laundering or terrorism financing.

687. According to the FATF definition, an NPO should be understood as a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"[331].

688. The European Commission detailed the scope of NPO activities, indicating that it includes:

- service activities that include programmes aimed at providing housing, social services, education or health care (that may consist, for example, in providing humanitarian or development aid, as well as conducting other types of activities),
- expressive activities, i.e. programmes focusing on sports and recreation, arts and culture, representation of interests or support, conducted, for example, by political parties, think tanks and advocacy groups (i.e. organisations generally engaged in philanthropy).

[331] Best practices – Combating the abuse of non-profit organisations (Recommendation 8), FATF, June 2015, p. 7, at: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html

689. The social sector in Poland consists of organisations that are not profit-oriented and are not an element of the Polish state structure, and are thus called NPO[332] or NGO[333].

690. In accordance with Polish law, this type of organisations includes primarily foundations and all types of associations. Pursuant to Article 3(2) of the *Act of 24 April 2003 on public benefit activities and volunteering* (Journal of Laws of 2023, item 571), foundations and associations are classified as non-governmental organisations and as such are subject to the regulations of this Act, which entitles them to apply for the status of a public benefit organisation or public administration subsidies.

691. Every association is an organisation in which the members of the association always enjoy the highest authority. To establish an association a group of people (at least 7 persons in the case of a 'registered association'[334] and at least 3 persons in the case of an 'ordinary association'[335]) is required. No assets are required to establish an association. Besides the aforementioned types, associations also include sports clubs, student sports clubs, and volunteer fire brigades.

692. In Poland, foundations and associations are registered in the National Court Register (KRS). During the registration process, a foundation and an association must, among others, submit information on its organisation to the Central Register of Beneficial Owners (within 14 days from the date of establishment of the association) and have its own bank account. To establish a 'registered' association, the following requirements must be met: 7 persons and the association's statute – written information regarding the rules for the association's operation. In the case of establishing a foundation, a founder that allocates certain property for a publicly useful purpose is required. A founder may be both a Polish citizen and a foreigner because, in accordance with Article 2(1) of the Act, "a foundation may be established by natural persons regardless of their citizenship and place of residence". A foundation may also be established by a legal person (e.g. a university, private company) established in Poland or abroad. There may also be several founders – several natural persons, several legal entities or a group of both natural and legal persons. The purpose of the foundation's operation should be socially or economically useful.

693. A total of 138 thousand non-governmental organisations (107 thousand associations (excluding volunteer fire brigades) and 31 thousand foundations[336]) are registered in Poland. Not all registered organisations actually conduct their activities – according to Statistics Poland, approx. 50% of those listed in the register actually operate. The others have suspended or terminated their activities, but have not deregistered. It can therefore be estimated that approx. 70 thousand non-governmental organisations (excluding volunteer fire brigades) operate

[332] non-profit organisation – a non-governmental organisation whose activities are not aimed at bringing profit to the bodies managing it. It is financed from public budgets: state, regional and local ones

[333] non-government organisation – an organisation that works for a selected interest and does not act in order to make a profit

[334] A registered association has legal personality, can establish local organisational units, join associations, accept legal persons as its members, benefit from public donations and accept subsidies from state authorities and other institutions. The issue of establishing this type of associations is regulated by Chapter 2 "Establishment of associations" of the Act – Law on Associations of 18 November 2020. (Journal of Laws of 2020, item 2261).

[335] Ordinary association – a form of simplified association. It does not have legal personality, and its establishment requires only three individuals who must adopt regulations (thus not a statute) and designate the association's representative. Issues regarding ordinary associations are listed in Chapter 6 of the Act – *Law on Associations* of 18 November 2020.

[336] Statistics Poland, REGON statistical register, as at the end of 2021

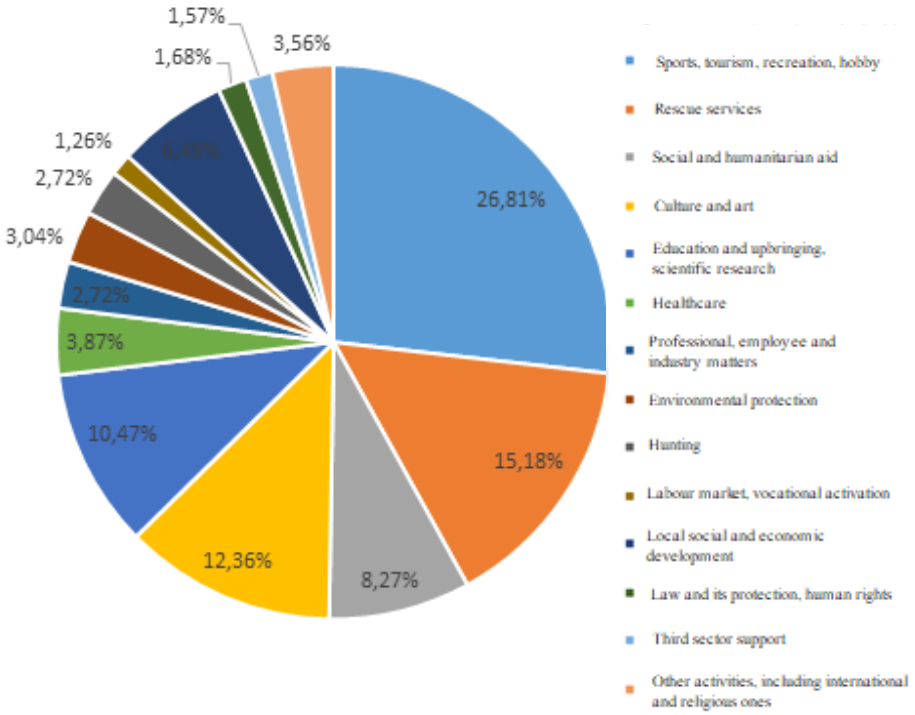
actively in Poland. Registered non-profit organisations are characterised by their significant diversity in terms of the areas in which they conduct their statutory activities. According to Statistics Poland[337], in 2020, the largest number of these entities indicated sports, tourism, recreation and hobbies as their primary areas of activity (25.6 thousand entities), of which 70.5% were sports associations. The second largest group consisted of entities conducting rescue activities (14.5 thousand organisations) – volunteer fire brigades and other volunteer rescue organisations (Volunteer Water Rescue Service, Polish Volunteer Mountain Rescued Service). *Table 28. Number of registered non-profit organisations by primary area of activity (in thousands)*[338]*:*

Sports, tourism, recreation, hobby	25.6
Rescue services	14.5
Social and humanitarian aid	7.9
Culture and art.	11.8
Education and upbringing, scientific research	10.0
Health care	3.7
Professional, employee and industry matters	2.6
Environmental protection	2.9
Hunting	2.6
Labour market, vocational activation	1.2
Local social and economic development	6.2
Law and its protection, human rights	1.6
Third sector support	1.5
Other activities, including international and religious ones	3.4

Chart 21. Number of registered non-profit organisations by primary area of activity (in percent)

[337] Statistics Poland report of 2022 (information prepared every two years): Sektor non-profit w 2020r. Stowarzyszenia, fundacje, społeczne podmioty wyznaniowe, samorząd gospodarczy i wyznaniowy (The non-profit sector in 2020. Associations, foundations, social religious entities, economic and religious self-government), https://stat.gov.pl/wyszukiwarka/?query=tag:organizacje+non-profit

[338] Ibidem

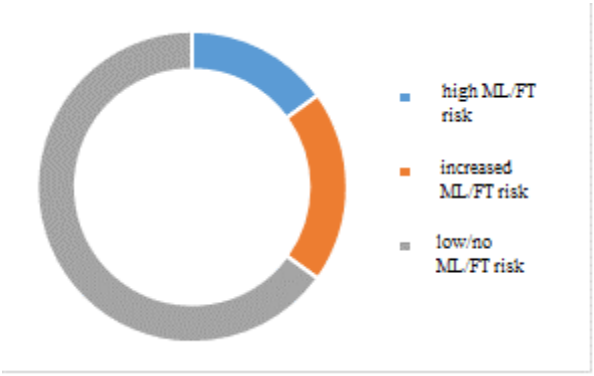


694. In accordance with the FATF Recommendations, non-profit organisations are characterised by varying degrees of risk depending on the type and form of the foundation or association.
Within specific ML/FT risks, the FATF distinguishes certain non-profit organisations according to the degree of ML/FT risks characterising a given entity (foundation, association). It should also be noted that in accordance with its definition of a non-profit organisation (see above), the FATF lists specific organisations, such as charitable, religious, cultural, educational, social or carrying out other types of "good works" – FATF definition[339]. The indicated definition is therefore narrow and refers to the spectrum of entities defined as non-profit organisations.

695. According to FATF Recommendations[340] certain types of foundations and associations may be more susceptible to criminal activities, such as terrorism financing or money laundering. According to available international information and the GIFI's experiences, it can be concluded that non-profit organisations susceptible to criminal activities include, for example, entities operating internationally and those engaged in religious activities (high ML/FT risk), entities carrying out activities related to social and humanitarian aid (increased ML/FT risk), and others (low/no ML/FT risk[341]). At the same time, it should be emphasised that the ML/FT risk of a given type of foundation and association may change depending on ML/FT factors.

[339] Best practices – Combating the abuse of non-profit organisations (Recommendation 8), FATF, June 2015, p. 7
[340] International standards on combating money laundering and financing of terrorism & proliferation, p. 58
[341] Non-profit organisations that do not generate ML/FT risk include rescue services – e.g. volunteer fire service.

Diagram 3. Types of non-profit organisations by the ML/FT risk generated by them



696. Based on the data held by the GIFI (for 2020-2022) relating to money laundering and terrorism financing, it is worth paying attention to several examples relating to criminal activities identified in the aspect of the operation of associations and foundations.

697. In 2022, the GIFI submitted a notification to the prosecutor's office regarding money laundering by defrauding non-profit organisations of funds that were probably intended for food for refugees from Ukraine. Ultimately, the funds were transferred to companies with personal and capital links with the defrauders as "loans" or "shareholder subsidies". In 2022, the prosecutor's office initiated an investigation into the case.

698. In 2021, the GIFI received a notification from a payment institution regarding a foundation that carried out financial transactions with high risk countries. The obligated institution also noticed an unusual, high volume of rejected financial transactions (multiple of 100) involving the aforementioned foundation, and the amounts of financial transactions that in many cases exceeded USD 1,000. The foundation's activities included, among others, psychotherapeutic support for children, adolescents and adults who have experienced a traumatic event (post-traumatic stress, trauma victims). Based on the collected materials, the GIFI concluded that the bank accounts kept for the foundation were used to launder money, probably from unauthorised payment card transactions. The competent prosecutor's office initiated an investigation in the case concerned.

699. Another case regarding a foundation was recorded in 2020. An obligated institution (bank) provided the GIFI with information regarding suspicious financial transactions carried out by natural persons (from abroad) to credit the accounts of this foundation. These funds were related to the laundering of money defrauded from misled natural persons using a financial platform operating without the authorisation of a foreign supervisory authority under the guise of depositing funds for a product called CFDs (contracts for difference – on raw materials, indexes, shares and currencies). The funds were ultimately transferred to foreign companies to accounts kept, among others, with Cypriot banks. The competent prosecutor's office initiated an investigation into the case in question.

700. In 2020, the GIFI sent a notification to the prosecutor's office regarding suspicious financial transactions made by 4 entities – associations. The aforementioned entities indicated *activities of religious organisations* as the main subject of their economic activity. Pursuant to the *Act on tax on goods and services*, churches and religious associations are exempt from the obligation to pay VAT. Moreover, under the *Corporate Income Tax Act*, the aforementioned

entities were exempt from CIT (income of church legal entities from non-economic statutory activities). In this case, the entities concerned were actually engaged in other economic activities, i.e. construction works (construction of residential and non-residential buildings). No taxes were paid to the state budget on this account. The funds were then transferred from bank accounts denominated in various currencies to an online currency exchange office to make it difficult to identify their source. The funds were ultimately transferred to entities established, among others, in Asian countries. The competent prosecutor's office initiated an investigation into the case.

701. According to the 2021 Report entitled *"Kondycja organizacji pozarządowych"*[342] (*The condition of non-governmental organisations)* over half (54%) of non-governmental organisations carries out activities[343] relating to sports, tourism, recreation and hobbies, e.g. they conduct sports activities and organise recreational events. More than half of the organisations (51%) deal with education. Compared to 2018, the number of organisations dealing with education has increased (an increase of 3% in 2021[344] /51%/ compared to 2018 /48%/). This may have been due to the period of the COVID-19 pandemic, when many organisations that had not previously specialised in this area began to support distance education. Every third organisation (34%) undertakes activities in the area of culture and art, and every fifth (19%) deals with health care. Looking at the changes between 2018 and 2021, it is worth paying attention to the increase in the number of organisations that carry out activities related to ecology and the environment, e.g. by engaging in education regarding sustainable development or activities to increase awareness of the threats related to the climate crisis. The percentage of organisations dealing with preserving and promoting national identity has also slightly increased (from 11% in 2018 to 13% in 2021). Although this area includes both activities for national and ethnic minorities and the regional language, as well as the preservation of Polishness and the development of national, civic and cultural awareness, the latter category (preservation of Polishness) definitely prevails in the group of organisations operating in this sector (increase from 11% to 13% in 2018-2021). A similar increase as that recorded in the area of preserving national identity is observed in the "international activities" and "religion" sectors (in both cases, an increase from 2% in 2018 to 4% in 2021 was recorded).

702. The aforementioned Report includes also information on the scale of activities carried out by non-profit organisations: 39% of them operate as local organisations, 24% of them are regional organisations, 28% of them are nationwide organisations, and 9% of them are international organisations.

703. From the point of view of the operation of non-profit organisations, data on the average annual income of such organisations is also important. According to the said Report, their average 2020 income amounted to PLN 26,000.

704. Pursuant to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, associations with legal personality and foundations established under the law on foundations or associations become obligated institutions where they accept or make cash payments with a total value equal to or exceeding EUR 10,000, regardless of whether such

[342] https://fakty.ngo.pl/raporty/kondycja-organizacji-pozarzadowych-2021. This report indicates, among others, qualitative and quantitative changes between 2018 and 2021.
[343] Both associations and foundations often operate in many areas at a time, e.g. sports and education
[344] The study was conducted in January 2022.

payment is made as a single operation or several operations that seem to be related to each other.

705. According to the European Commission, possible scenarios related to raising and transferring funds through NPOs include:

- creating an NPO to "raise funds" – funds from criminal activities are gradually transferred to this organisation (that may be used to support a specific criminal group or terrorist organisation by outsiders, i.e. people from outside the NPO, or by insiders, i.e. people operating within the NPO),
- using operating NPOs to finance local terrorist activities or to facilitate international transactions in order to transfer funds to areas where NPOs operate close to areas of terrorist activities (in this case, the organisation may also be used to support a specific terrorist organisation or criminal group, by outsiders or insiders).

706. The experience of the GIFI shows that NPOs can also be used for money laundering where they have no links with the activities of terrorist organisations and terrorism financing. The threat of using NPOs for money laundering results primarily from the following features of their activities:

- carrying out transactions with multiple entities – natural persons and legal entities (which includes accepting funds from both regular and random, one-off donors),
- using fund raising methods that facilitate the concealment of sources of funds' origin and the identity of actual donors (e.g. public fundraising, charity auctions),
- numerous types of transactions made, both cash and non-cash ones, sometimes also international ones.

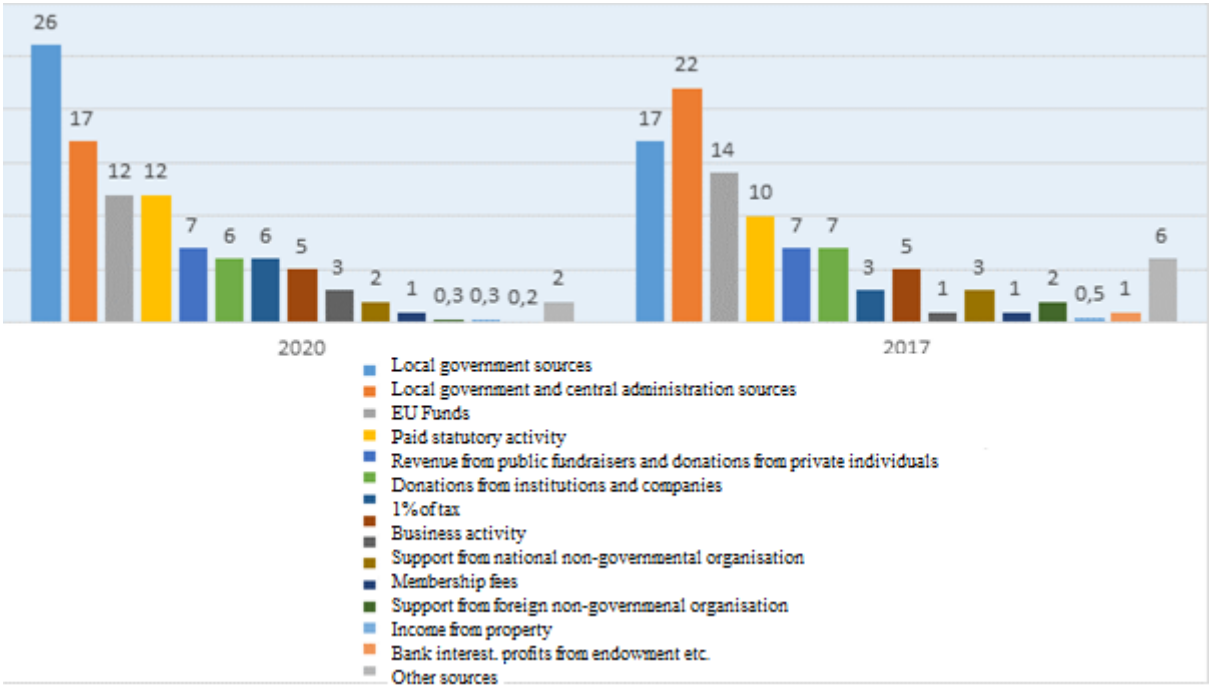
707. Foundations and associations may obtain funds from various sources, including:

- subsidies,
- paid public benefit activities,
- business activity, by selling services or products to achieve their statutory objectives (in this case they are obliged to register their business activity),
- public fundraisers,
- monetary donations and gifts in kind,
- sponsoring,
- charity auctions.

708. Organisations (foundations and associations) can finance their activities with funds from various sources. The number of types of revenue sources in an organisation's budget affects its financial standing – the more sources, the higher revenue is generated on average by a given organisation. According to the 2021 report entitled "*Kondycja organizacji pozarządowych*" (The condition of non-governmental organisations), most organisations use several funding sources (58% of them had no more than three funding sources). A detailed analysis of the numbers of revenue sources used by non-governmental organisations shows that in 2020 (compared to 2017), there was an increase in the percentage of both organisations with no more

than three types of sources (from 53% in 2017 to 58% in 2020) and those with more than six different funding sources (i.e. from 11% to 14%).

Chart 22. Percentage of organisations (associations and foundations) using particular sources in the sector budget in 2020 (comparison with 2017)[345]



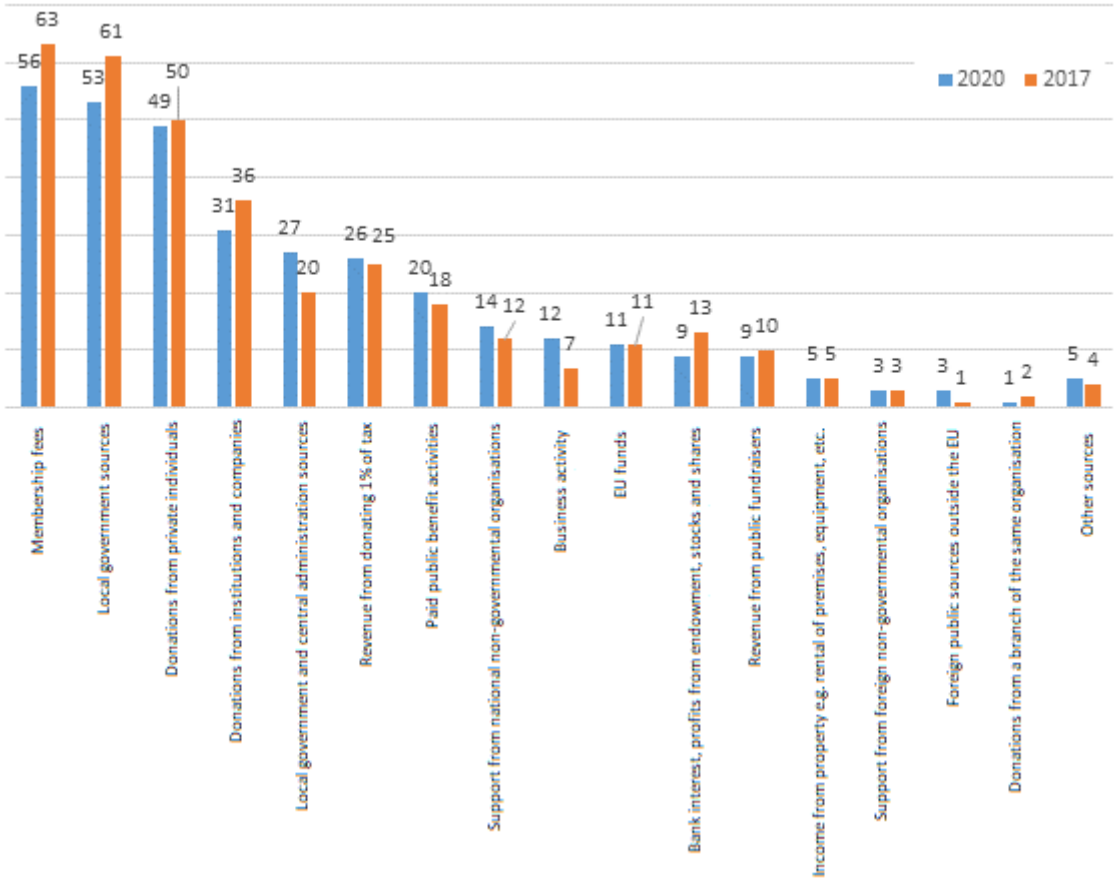
709. According to the aforementioned information, public sources remain the basic source of non-governmental organisations' income, and their importance even slightly increased (by 6% between 2020 and 2017). The percentage of revenue from economic activity and property, as well as from private and corporate philanthropy, remained at the same level as in 2017. However, the proportion of other sources decreased slightly (including membership fees, as well as sources not assigned to any of the aforementioned categories).

710. According to the analysis carried out by the Klon/Jawor association, a large part of NPOs uses various sources of obtaining funds. According to this data, the most frequently used revenue sources in 2020 included: membership fees, local government sources, and donations from private individuals as well as institutions and companies (see Chart 23 below).

Chart 23. Percentage of organisations (associations and foundations) using particular revenue sources in 2020 (comparison with 2017)[346]

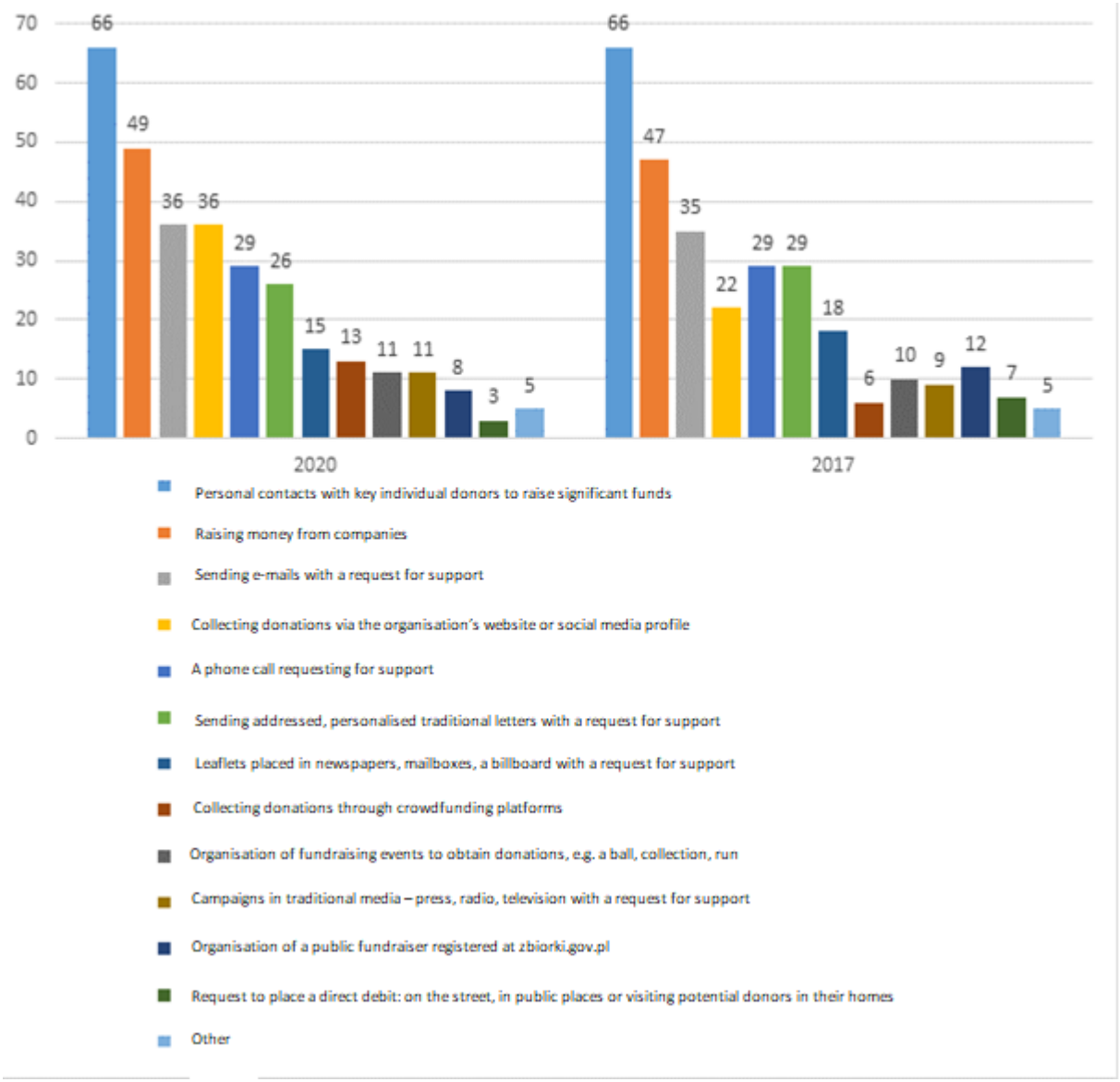
[345] Based on data from the report entitled *"Kondycja organizacji pozarządowych"* (The condition of non-governmental organisations) from 2021, p. 71, at: https://publicystyka.ngo.pl/nowosc-raport-kondycja-organyzacji-pozarzadowych-2021-zaangazowane-mimo-powiedznosci

[346] Ibidem.



711. In the case of associations and foundations, fundraising is also important. According to analyses conducted by the Klon/Jawor association, the activities aimed at obtaining funds included, like in 2017, primarily personal contacts with key donors (66%) and obtaining money from companies (49%). Raising donations via a website or social media profile is also increasingly popular (36%) – since 2017, the frequency of undertaking such activities has increased by 14 percentage points. An increase (by 7 percentage points compared to 2017) has also been recorded in the use of crowdfunding platforms – 13% (Chart 24 below).

Chart 24. Fundraising activities in 2020 and 2017



712. Numerous sources of fundraising make it possible to transfer assets from illegal activities to NPOs to be laundered. For example, funds generated through crime, paid as donations from straw men or non-existent natural or legal persons, may be then – legally – transferred to specific persons or business entities in line with the purposes specified in the organisation's statute.

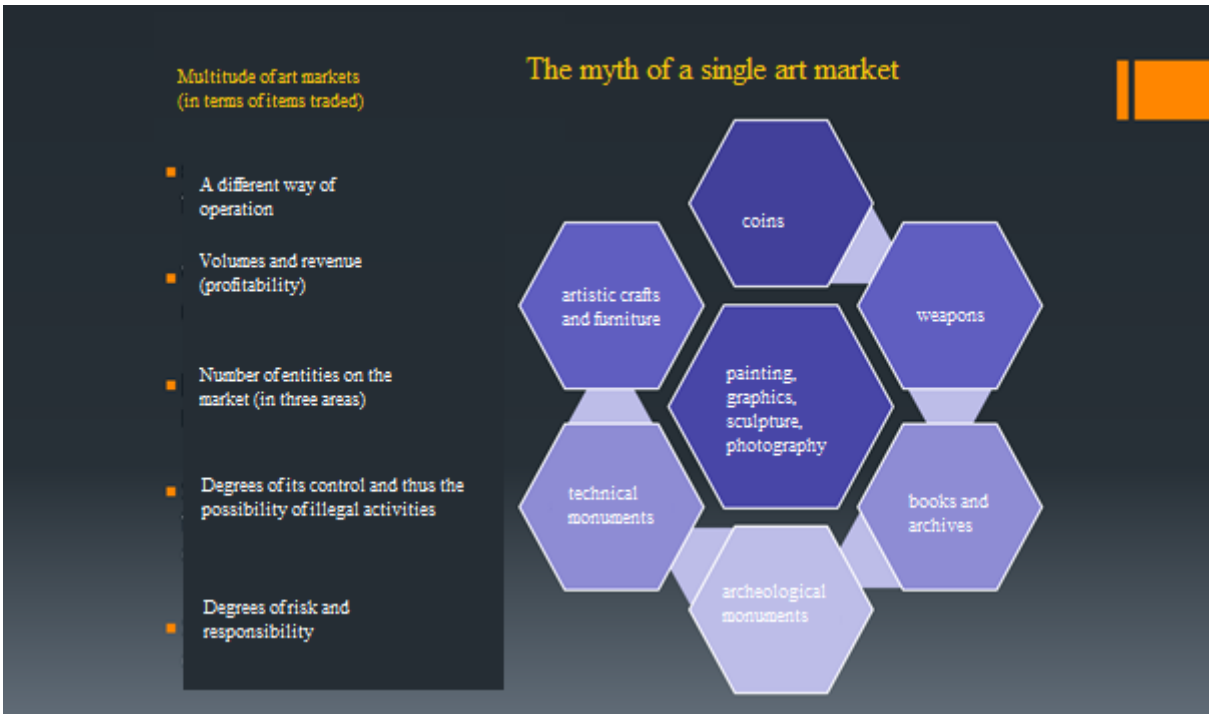
Trade in antiques and works of art

The structure of the art market in Poland and its overall characteristics

713. The art market in Poland is a domestic market that should be classified in terms of *entities* operating on it (sellers, agents and buyers – foreign entities, natural persons and legal persons account for a small percentage of buyers) and *items* (Polish works of art or works of art related to Poland (painting segment) account for 80% of traded items).

714. The structure of the art market should be considered either from the perspective of items traded on this market[347] or that of entities operating on this market[348]. The former is related to the segmentation of the art market, i.e. distinguishing particular areas of this market according to traded items – i.e. painting, photography, sculpture, graphics, artistic crafts, furniture, etc. Based on this point of view, several market segments, i.e. bibliophilism, numismatics, technical monuments, antique weapons and archaeological monuments, have not been included in the descriptions below. Due to their numerous specific characteristics – primarily as regards entities involved (i.e. a specific group of agents – much more specialised and operating practically only in this market segment) as well as traded items (trade in old coins and trade in books is governed by specific rules that are different from those applied in other market segments, while trade in archaeological monuments or antique weapons is subject to specific restrictions under Polish law).

Diagram 4. The myth of a single art market



715. The structure of the art market should be considered primarily from the perspective of entities operating on it, focusing on: first of all, identifying the key entities on this market, and then on its classic division into the *primary* and *secondary* market.

716. *The primary market (called the gallery market)* – is related to the flow of works of art from artists' studios to galleries, and only then to further buyers (collectors, investors). In mature markets, artists are represented by specific galleries (often more than one with a regional division – in this case, a consignment system is often used). Therefore, the primary market

[347] Types of art that make up the market structure (trade in works of art).
[348] Information on particular entities trading in works of art and information on the forms and methods of trading in works of art.

should include both artists selling their works directly (regardless of the sales channel – in this case, studio sales, online sales, etc.), as well as galleries that represent artists and are responsible for placing a work of art on the market for the first time. Therefore, what qualifies a given entity to the primary market is not the name of the entity (gallery, antique shop, art lounge, etc.), but the activity of the entity itself. The primary market in Poland is currently much smaller (in terms of the generated turnover) than the secondary market and is largely concentrated in Warsaw. What is traded on it is naturally current art, through – apart from classic gallery sales – art fairs. In Poland, the primary market, like the Western European gallery market, started to be built again only around 2000, and over the last few years, galleries from other parts of Poland have been moved to Warsaw. On the other hand, these are entities – agents with smaller capital than those operating on the secondary market, mainly auction houses. The "strongest" players on the primary market include the Foksal Gallery Foundation and Galeria Raster.

717. *The secondary market* – often equated with *the auction market* – where works of art that have previously been traded are offered (the subsequent resale takes place not from the artist's studio, but from an art collector). Besides the activities of auction houses, the secondary market also includes the activities of antique shops and galleries (and other entities) that trade in works of art that have already been put on the market. Having regard to the advantage – in terms of turnover – of auction houses over antique shops, currently the strongest market players on the secondary market in Poland include: Desa Unicum, Dom Aukcyjny Polswiss Art, Agra-Art, and Sopocki Dom Aukcyjny. It is the auction market that is the most visible element of the art market for observers from other countries, unfortunately very often wrongly equated with the entire art market in Poland or interchangeably referred to as such.

718. The *auction market* in Poland: (a) is authoritative for formulating assessments and forecasts. It influences the overall image of the art market, (b) auctions of works of art are a social phenomenon on this market, they are an attractive form of reaching consensus, hence their extensive media attention, (c) is a kind of public market verification of artists, (d) enjoys greater public trust in the authenticity of items and price reliability[349], (e) has an impact on the gallery market and antiquarian market in various areas: price level, fashion setting, building interest (of collectors, investors, those who only begin their adventure with this market).

719. Over the last few years, the boundaries between the primary and secondary markets on the Polish art market have become increasingly blurred due to the rapid development of young art auctions or current art auctions (unseen to this extent on mature markets – looking at their percentage). This is caused by both the significant activity as well as the financial advantage of auction houses as an element of the secondary market over the primary market. The only emerging primary market in Poland is currently unable to "absorb" a significant number of new artists, which benefits the auction market that only sells the works of art they create.

720. The exact number of entities operating on the primary and secondary markets in Poland is unknown, even if we took into account only agents operating on these markets, thus excluding artists selling their works directly on the primary market – i.e. without the involvement of galleries, and in the case of secondary market – entities trading in works of art incidentally, i.e. "private sellers", although, as a rule, they carry out transactions that involve works of art, and

[349] In fact, this is a stereotype, because this market is not free from counterfeits, and it succumbs to and even develops its own market games that affect the price level.

are thus subject to tax on civil law transactions (Polish: *podatek od czynności cywilno-prawnych* – PCC). The available data in this respect shows substantial differences:

(1) in its reports, Artinfo.pl, includes only entities operating on the auction market (i.e. part of the secondary market), without providing data on the remaining part of the secondary market – i.e. the antiquarian market, not to mention the primary market, thus focusing on the number of entities that conducted at least one auction in a given year, e.g. 51 entities organising an auction in 2020 and slightly more in 2021. It is worth noting that Artinfo.pl reports do not include in this respect all entities conducting auctions, but only those that used the aforementioned platform;

(2) Statistics Poland indicates that the total number of entities – art dealers – thus both those operating on the secondary and primary markets, is approx. 200 (e.g. in 2021, this figure was 209);

(3) documents accompanying the legislative process – e.g. the Regulatory Impact Assessment (RIA) prepared in connection with the amendment to the *Act of 23 July 2003 on the protection and care of monuments*, as part of the proceedings of the *Act of 25 May 2017 on the restitution of national cultural property* (Journal of Laws of 2019, item 1591), indicated approx. 600 art dealers that would be obliged to keep a record (where, among others, transactions involving monuments worth more than PLN 10,000 are to be entered). Current art that is not classified as a monument is not subject to these restrictions, thus entities trading in such art were not included in the RIA;

(4) data provided by the *Scientific and Research Team for Trade in Works of Art and Legal Protection of Cultural Heritage*[350] indicates more accurately the number of art dealers in 2021 – 380 entities:

(a) number of entities operating on the primary market – 78,

(b) number of entities operating on the secondary market:

- auction houses/secondary market entities conducting at least one auction
- (the list does not include entities that conducted incidental charity auctions of works of art in a given year, for example auctions related to fundraising for Ukraine) – 89.
- other entities trading in works of art on the secondary market that did carry out auctions – 213.

Trade in cultural property[351] *on the Polish art market*

721. Trade in cultural property on the Polish market is characterised by:

(1) erroneous treatment of the art market as a market for luxury goods. This is the result of equating the art market exclusively with the auction market (with more extensive media attention), that is only one of the elements of the former and has an impact on the

[350] Data provided by the Scientific and Research Team for Trade in Works of Art and Legal Protection of Cultural Heritage (under the supervision of Prof. W. Szafrański), Faculty of Law and Administration, Adam Mickiewicz University in Poznań.
[351] The concept of "cultural property" covers the category of both monuments and works of art that are not monuments.

antiquarian market or the gallery market that are completely different (operate under different rules), hence the interests of even these three types of entities (not mentioning others) on the market (auction houses, antique shops and art galleries) are not the same;

(2) uncritical trust of buyers (e.g. carelessness about the provenance of items) in dealers as professionals;

(3) buyers' unawareness of the lack of supervision over the market (thus, buyers very often side with the dealer, considering that the secrecy standard is the specific characteristics and tradition of the art market);

(4) lack of supervision over auction quotations, which means that the lists of such quotations also include works of art that have not actually been sold (no transaction) as well as conditional quotations, without verification whether the transaction has taken place or not, etc.;

(5) erroneous recognition of the art market as strong in terms of capital, especially with respect to those dealing on this market. The secondary market is dominated by consignment sales. Individual dealers are able to build up warehouse stocks of works of art intended for future sales;

(6) lack of contracts perceived as the standard of the Polish art market (including private sales without 2% tax on civil law transactions), no invoicing, cash transactions (on the largest scale in the area of cultural property worth up to PLN 100,000);

(7) belief that being honest on the art market does not pay, hence the economic failure of entities with greater trading transparency that lose with unfair competition using illegal market games;

(8) frequent investment of untaxed or illegally obtained funds in cultural property/works of art;

(9) ease of price manipulation – lack of control in this area (prices affect museum purchases, insurance, deposits) – levels of future prices (as determinants of estimated prices of subsequent works);

(10) lack of "thread" control underlying the introduction of "record books" into the Polish legal system (these regulations are included in the *Act on the protection and care of monuments*);

(11) uncertainty of the state authorities themselves – fear of making a mistake in activities on the art market – lack of expert support.

722. The aforementioned differences regarding entities operating on the art market, from the perspective of those dealing in works of art, also mean that in terms of turnover on the Polish art market, this data is more estimated than absolutely certain. Artinfo.pl reports showed the following turnover on the auction market in particular years: in 2019 – PLN 294.9 million, in 2020 – PLN 380.4 million, in 2021 – PLN 634.1 million, in the first half of 2022 – no data (the report will be published in 2023). The Artinfo.pl report does not present any other information regarding other elements of the art market.

723. Statistics Poland data also includes sales of works of art outside auctions. But even in this case, the adopted, specific method of information analysis does not allow easy comparison

of this data with data from Artinfo.pl. Statistics Poland presents data from the market, breaking it down into turnover from traditional auctions and turnover from online sales. It can thus be understood that part of auction sales, i.e. online auctions of auction houses, are included in this last part, along with the sales made by galleries and antique shops, that also partially sell their goods via the Internet. According to Statistics Poland, the detailed turnover related to works of art in Poland in the period concerned amounted to:

(1) art market 2019 – PLN 162.5 million = PLN 75.4 million (traditional auctions) + PLN 64.1 million (sales in retail outlets) + PLN 16.8 million (online sales);

(2) art market 2020 – PLN 418.5 million = PLN 266.7 million (traditional auctions) + PLN 88.7 million (sales in retail outlets) + PLN 58.4 million (online sales);

(3) art market 2021 – PLN 591 million = PLN 381.9 million (traditional auctions) + PLN 141.3 million (sales in retail outlets) + PLN 59.2 million (online sales);

(4) art market H1 2023 – no data.

724. Comparison of data regarding traditional auctions presented by Statistics Poland for 2019 and that presented by Artifno.pl for the same year is quite puzzling given a difference of PLN 219.5 million (PLN 294.9 million according to Artinfo.pl and PLN 75.4 million according to Statistics Poland). According to Statistics Poland data, the entire art market in 2021 generated turnover of PLN 591 million, while according to the Artinfo.pl report, the auction market itself (having regard to the reservations indicated above) amounted in 2021 to PLN 634.1 million.

725. The data provided by Scientific and Research Team for Trade in Works of Art and Legal Protection of Cultural Heritage:

(1) art market in 2019 – PLN 467.5 million = PLN 311.2 million (turnover of auction houses) + PLN 156.3 million (turnover generated by antique shops and galleries operating on the primary and secondary markets);

(2) art market in 2020 – PLN 561.8 million = PLN 398.7 million (turnover of auction houses) + PLN 163.1 million (turnover generated by antique shops and galleries operating on the primary and secondary markets);

(3) art market in 2021 – PLN 838.6 million = PLN 651.2 million (turnover of auction houses) + PLN 187.4 million (turnover generated by antique shops and galleries operating on the primary and secondary markets);

(4) art market H1 2022 – the turnover amount in the case of auction houses was PLN 272.8 million. Data from other segments of the art market is not available. Based on data for H1 2022, of the largest entities on the auction market, only Desa Unicum recorded slightly better results than in H1 2021 – the other three largest auction houses, i.e. Polswiss Art Dom Akcyjny, Agra Art, Sopocki Dom Aukcyjny, recorded turnover that was either similar or slightly worse than in H1 2021

726. As regards the indicated turnover of auction houses, the aforementioned Scientific and Research Team also took into account the auction results of those auction houses that did not conduct their auctions via the Artinfo.pl platform. The Scientific and Research Team also tried to verify and then take into account data regarding transactions that took place outside the auctions themselves.

727. Attention should also be paid to the sales of other art dealers (besides auction houses). A fundamental question arises as to how to treat them, given that many antique shops/galleries operating on the secondary market are the main suppliers of items for auctions on the Polish art market, while auction houses go on tours around galleries, preparing subsequent auctions. Some antique shops also report transactions in which the antique shop is the seller at an auction to be included in the Statistics Poland records. At the same time, auction houses show such sales in their turnover, which may result in the duplication of sales turnover. It is also known that antique shops often show, for example, when responding to Statistics Poland inquiries, only their margin (sometimes understating it). They also do not disclose turnover when they sell works of art to clients they know (e.g. they do not enter such items in their record books). This is the aftermath of the fact that the Polish art market has "adopted" the form of non-contractual sales of works of art, treated as a type of market culture.

728. What is an important issue in the art trade industry is the lack of any regulations regarding documents on the art market and liability on this account, which results, among others, from the lack of expert market regulation in Polish law (except for the experts of the Minister of Culture and National Heritage). This leads to the development of discretionary documents and various types of certificates that are not regulated by law.

729. It should be added that the data presented above does not include the so-called private sales, i.e. incidental sales of works of art (that, in principle, should be subject to tax on civil law transactions), and other elements of the shadow economy in this area, e.g. trading works of art by the so-called "activists" (a jargon term used on the Polish art market to refer to entities that make a living trading works of art, but do not conduct any form of economic activity in this field). Formally, they should be treated as economic operators, but they remain out of reach for state authorities). This group, and thus the turnover, includes illegal trade in works of art. Estimates in this respect are very difficult to determine; the model assumes that in Western European markets this is approx, 1/3-1/4 of "legal turnover". In Poland, it would probably be much less.

730. Varied data regarding both the entities on the art market and the levels of turnover may suggest certain shortcomings in the method of supervising the art market, regarding, among others, information on obtaining data from this industry. In this respect, the activities of the GIFI, and to some extent also the National Revenue Administration, are gaining new importance due to the tasks imposed on these entities by the legislator, or "equipping" these entities with "competence" to act on the art market (resulting from both AML aspects and regulations regarding record books).

731. The art market is perceived on a global scale as one of the markets generating the largest illicit revenue, next to the arms market, human trafficking and drug trafficking. It is quite different from the "markets" mentioned above, becoming an increasingly "attractive" sector for broadly understood crime. e.g.: high profits with relatively low risk, low market flexibility (price increases do not suppress demand on the market), limited number of works of art, existence of a legal market with a lower level of state control, complexity of criminal policy instruments relating to this market, consent of participants of the legal market to "underground" activities of other entities, as well as a different structure and understanding of organised crime on this market.

732. The Polish art market is part of the international art market. It should be noted that the domestic market is small considering the scale of global turnover in this sector (it constitutes little more than one per mille of a percentage of global turnover), but its systematic growth can be seen, regardless of the economic situation in Poland. It should also be noted that two Polish auction houses have a turnover at a level that ranks them among the top 10 and 15 auction houses operating in Europe.
These are: Desa Unicum (the first 10 auction houses in Europe) and Dom Aukcyjny Polswiss Art (the first 15 auction houses in Europe).

733. In Poland, there are currently no legal regulations aimed directly and comprehensively at the art market (lack of the so-called "heritage catalyst"), which results in a situation where many different state bodies and institutions, sometimes acting on general terms, and rarely under special regulations, i.e. ones relating exclusively to the art market, take action that affects the broadly understood art market or trade in cultural goods.

734. The art market in Poland has been developing over the last 30 years. The short – compared to Western European countries – period of this market's operation in Poland is measurable, but the mechanisms that have developed therein are often different from those occurring in mature markets. It should be noted that already at the initial stage of the development of the art sector market in Poland, there was a rapid loss of its transparency and a violation of two elementary principles of its proper operation, namely the authenticity of traded items and price credibility. There is no doubt that this transparency will have to be gradually restored using hard law (i.e. the legislator's actions facilitating the elimination of undesirable phenomena on the art market) as well as soft law (developed by professional organisations or institutions associating buyers or sellers, emerging on the domestic art market).

735. The art market in Poland and the trade in cultural property are monitored by the following law enforcement agencies: the Police, the Prosecutor's Office, the National Revenue Administration, the Central Investigation Bureau of the Police, the Internal Security Agency and the Central Anti-Corruption Bureau. In 2019 - 2022, certain activities of state authorities on the art market were recorded, including:[352]:

(1) the Galleri New Form case conducted by the Internal Security Agency in Białystok and the Regional Prosecutor's Office in Białystok – allegations of money laundering and the creation of a pyramid scheme based on trade in works of art (the proceedings have been pending since 2018);

(2) conducting an investigation by the Central Anti-Corruption Bureau (Branch in Katowice) together with the Voivodeship Police Headquarters in Katowice under the supervision of the Circuit Prosecutor's Office in Gliwice, in connection with the suspicion of committing a prohibited act, among others, under Article 299(5) of the Penal Code (charges under Article 299(1) were brought against 8 suspects in the case). The investigation in question covered defrauding educational subsidies and siphoning funds from companies. The thus obtained funds were then invested in 2019 - 2021, among others, in works of art (paintings). The total amount of cash spent on works of art in this period was PLN 652,200;

[352] The data provided by Scientific and Research Team for Trade in Works of Art and Legal Protection of Cultural Heritage (led by Prof. W. Szafrański), Faculty of Law and Administration, University of Adam Mickiewicz in Poznań

(3) analytical proceedings initiated by the GIFI in 2020 included, among others, a case regarding illegal trade in works of art. Persons from Poland and Ukraine operating within organised criminal groups were involved in this case. In 2020, a Police body informed the GIFI that in connection with the proceedings supervised by the prosecutor's office, as part of which the GIFI sent a notification to the prosecutor's office, gold products and works of art (icons) for a total amount of PLN 1 million were seized during the activities performed;

(4) actions of the Office of Competition and Consumer Protection in 2022 clarifying whether auction houses in Poland violated the collective rights of consumers or used abusive clauses in contracts. The clarifications procedures covered auction houses, i.e. Agra-Art, Desa Unicum, Dom Aukcyjny Polswiss Art, Dom Aukcyjny Rempex, Sopocki Dom Aukcyjny.

736. The most commonly identified offences against movable cultural property in the activities of law enforcement agencies in Poland include: theft (burglary), artnapping (theft of works of art in order to extort a ransom for their return), mugging (robbery, extortion racket), appropriation, intentional and unintentional fencing of stolen goods, smuggling – illegal export and import (of monuments/cultural property), fraud involving cultural property, destruction of a monument, counterfeiting, processing (forgery) of a monument and placing it on the market – in the latter case, however, organised actions of competent authorities are necessary, because generally only single successful cases in this area deal with by the Police/prosecutor's office can be indicated, sometimes due to objective difficulties regarding evidence, sometimes due to errors and improper preparation for this type of highly specific and capital-intensive cases.

737. There are also other categories of offences on the art market, such as bribery through the art market, of which entities operating on this market (mainly dealers) are or are not aware, corruption on the art market in order to authenticate works of art (both fakes and those derived from crime), money laundering through the purchase (or sale – "whitewashing") of monuments/cultural property, illegal transactions on the art market understood as: trade in monuments/cultural property constituting *res extra commercium* (at the time of ratifying the convention, e.g. belonging to the underwater archaeological heritage), trade in monuments/cultural property being the subject of crime, i.e. simple fencing of stolen goods (e.g. from theft, counterfeits), trade in monuments/cultural property whose trade is restricted while abusing these restrictions (e.g. archaeological monuments), violation of foreign exchange regulations (e.g. cash payments abroad for cultural property, without declaring export of a total amount exceeding EUR 10,000), depleting customs and tax liabilities related to the import of cultural property/monuments to be further traded, by falsifying attributions or lowering their value, fake auctions and directed auctions – classified depending on the actual situation as, e.g. fraud, bid collusion, price inflating by the use of illegal market games, e.g. chandelier bidding, collusion of buyers, collusion of sellers, speculative games aimed to falsify or show false auction results and the quantitative level of sales, which consequently affects the level of future prices, obtaining proprietary information or personal data of market participants, creating speculative bubbles and pyramid schemes.

738. Illegal activity on the art market is also related to legalising works of art, i.e. authenticating works of art contrary to their actual assessment (authenticating the subject of the transaction) through opinions, museum exhibitions, false provenance/attribution activities,

confirming untruths in assessment and valuation documents, falsifying data and producing false analyses of the art market or its segments in order to make changes on the market (e.g. takeovers), falsifying expert opinions, which occurs less frequently in Poland than in Western European countries because there is no legal model of an expert opinion or expert market in Poland, and the liability of an "expert", due to the possible use of ambiguous (as regards content) expert opinions, allows for avoiding liability more easily than in the case of falsifying an expert opinion, underestimating – for tax purposes – the value of cultural property imported and sold by dealers, tax avoidance – concealment or intentional understatement of income by art dealers, conducting by auction houses closed auctions and not disclosing the income obtained therefrom, failure to verify by operators specialising in trade in cultural property whether the buyer and seller are included on the EU sanctions lists (e.g. in connection with the war in Ukraine).

Non-fungible tokens (NFT) on the Polish art. market

739. NFTs[353] are a new digital instrument, also used on the contemporary art market. NFTs are used, among others, for selling digital works of art. These are often 3D models, animations, music videos and multimedia forms that in most cases cannot be turned into any material form, as in the case of photos and two-dimensional graphics. An NFT with a unique certificate saved on the blockchain allows for buying and selling this type of digital works of art. The amounts resulting from the sale of NFTs may exceed multiples of PLN 1 million. Importantly, NFTs have not yet been covered by specific statutory regulations, either in Poland or the EU. This gives rise to certain investment risk, which requires NFTs to be treated as speculative financial instruments. The NFT market is estimated to have exceeded USD 40 billion in 2021[354]. NFTs can be purchased on dedicated exchanges. To purchase an NFT, one should choose which market to buy from and find out what type of digital wallet is required to store it and what type of cryptocurrency will be used to make the purchase. Currently, most NFTs are sold for Ethereum (ETH). The purchase process itself is still very complicated for most users who have no experience with, for example, digital wallets and cryptocurrencies. Purchasing an NFT requires setting up several accounts, including in a digital wallet application and on the chosen NFT exchange. Then, these accounts should be connected with each other and credited with an adequate amount of money to purchase a portion of Ethereum (or another cryptocurrency) for which the token will be bought. Some exchanges also charge an additional "gas fee" to compensate for GHG emissions that accompany each Ethereum-related operation. This fee can be up to several hundred zlotys.

740. NFT auctions quickly moved beyond the Internet. Christie's auction house[355] sold a digital collage of photos by Mike Winkelmann[356], aka Beeple, in an *.jpg file, in March 2021 for USD 69 million. The financial transaction was made using Ethereum.

741. It should also be emphasised that online creators of NFT tokens are frequently anonymous, which may lead to the creation of NFT tokens by unauthorised persons or those

[353] Non-fungible token (NFT) – a unique, digital unit of data based on blockchain architecture that can be traded between the protocol users, representing a wide range of tangible and intangible items, such as collectible sports cards, virtual real estate and virtual works of art.
[354]https://www.bloomberg.com/news/articles/2022-01-06/nft-market-surpassed-40-billion-in-2021-new-estimate-shows
[355] https://pl.wikipedia.org/wiki/Christie%E2%80%99s
[356] https://en.wikipedia.org/wiki/Mike_Winkelmann

related to organised crime. Moreover, persons involved in this type of transactions are not registered anywhere. At the same time, the method of executing transactions using Ethereum makes it difficult to identify the parties to financial operations.

742. In terms of dealers/sellers, NFTs on the Polish art market can actually be divided into three groups: (1) those sold, and previously created directly by Polish artists – in this case the prices are usually not very high, and the buyers include mainly foreign collectors. Distribution channels include the Internet and social media, that are also used to drum up interest in such tokens, (2) those sold by galleries – NFTs created in consultation between the artist and the gallery, (3) those sold at auctions – by auction houses that also sell traditional art (the first auction house to sell an NFT was Artinfo that sold Tomasz Górnicki's NFT – "Fortune", on 28 November 2021. The highest auctioned NFT was one by Paweł Kowalewski, sold for PLN 552,000 at Desa Unicum.

743. As regards NFT sales by the top five auction houses in terms of turnover, their greatest number was sold by Dom Aukcyjny Agra Art. There are also new auction houses specialising in digital art, but they have not recorded any spectacular NFT sales in recent years.

744. Art in the NFT area can also be divided according to its nature/type, i.e. (1) the work of art exists physically, and at the same time an NFT has been made for it. Both works of art can be linked to each other, and therefore the NFT is a type of confirmation of authenticity and should be sold together with the physical work based on which the NFT was created. (2) The work of art exists physically, and at the same time an NFT was made for it, "separating" it, however, from the physical work of art that can no longer be traded because, for example, it has been transferred to a museum. Therefore, the turnover may only concern the NFT itself (e.g. Tomasz Górnicki's work entitled "Fortune" of the "Outer dark" series, sold on 28 November 2021 – the first NFT work of art sold at an auction in Poland (for PLN 312.7 thousand). The physical work of art was to be transferred to the Silesian Museum and thus be excluded from trade on the art market. It is also possible to collect physical works of art, turn them into NFTs and sell them, without the option for selling the collected physical works (in the form of a closed deposit). (3) The work never existed physically, and only an NFT digital work of art is being created. (4) The work used to exist physically, but was destroyed and is only being recreated in the NFT format (e.g. Paweł Kowalewski's work entitled "Dlaczego jest raczej coś niż nic" (Why is there rather something than nothing) – Desa Unicum auction – the NFT work of art sold for the highest price at an auction in Poland).

745. Besides its innovative form, NFT art also poses threats on the art market. These include: (1) NFTs are bearer instruments that codify ownership of a unique digital asset, (2) NFTs do not have a volatile exchange rate because they are considered unique – (subjective fluctuations in the value of a given NFT), (3) digital art assets are inherently easier to transfer between parties to the transaction than traditional works of art because in most cases the parties do not have to physically transfer the work of art or pay for shipping services, such as insurance, transportation or customs, (4) NFT platforms differ in structure, ownership and handling. Each of them often operates in a different way and, in many cases, has different due diligence standards or protocols. It should be noted that it is not possible to carry out due diligence if transactions are carried out quickly one by one, (5) a large number of virtual exchanges that also operate on the NFT market may develop their "own money laundering".

Business entities registered in tax or financial havens

746. Proceeds from crime are often invested and laundered in tax havens. The key characteristics of tax havens include: offering favourable terms and conditions for running a business or investing capital through exemption from income taxes, granting tax relief, guaranteeing security of business activity as well as anonymity used by investors. According to the OECD definition, a tax haven is a country that arranges its law in such a way that the conditions for doing business are attractive to specific countries. This concerns primarily setting very low taxes and unclear tax regulations, as well as the possibility of taxing income in this country without conducting business on its territory. Tax havens also include countries that are reluctant to cooperate in the exchange of tax information.

747. Tax havens enable taxpayers to avoid and evade paying taxes in their own country. Since 2017, the Council of the European Union has been publishing a list of non-cooperative jurisdictions for tax purposes. It is reviewed twice a year and the purpose of its publication is to help Member States fight tax fraud and tax avoidance. The latest EU list of non-cooperative jurisdictions for tax purposes was updated by the EU Council on 14 February 2023[357]. In Poland, the *Regulation of the Minister of Finance of 28 March 2019 on the determination of countries and territories applying harmful tax competition in the field of personal income tax* (Journal of Laws of 2019, item 600)[358] applies in this respect.

748. Besides typical tax havens, there are also "special" financial havens that offer specific benefits as regards administrative, financial and other intangible services and are characterised by strict protection of data subject to banking secrecy. Financial havens, just like tax havens, are located practically in all corners of the world, which allows easy access to them. These are usually small territories located on islands, often with a small population, underdeveloped industry and scarce or no natural resources, thus they take action to encourage potential investors to invest capital in their territory.

749. From the point of view of financial transactions concluded with entities registered in tax havens haven transactions are important. These are transactions concluded with entities (haven entities) that have their place of residence, registered office or management in a territory or in a country applying harmful tax competition (direct haven transactions) and transactions concluded with entities that are not haven entities, but the beneficial owner of a given transaction. In other words, transactions are made with a haven entity's agent (indirect haven transactions). In the case of making tax transactions, Polish taxpayers are obliged to prepare local transfer pricing documentation[359].

750. Solutions relating to financial crimes, tax evasion and tax avoidance are described in the EU document entitled "Report on financial crimes, tax evasion and tax avoidance" European Parliament resolution of 26 March 2019 on financial crimes, tax evasion and tax avoidance (2018/2121(INI)[360]. The aforementioned EU report describes specific directions of planned

[357]https://www.consilium.europa.eu/pl/policies/eu-list-of-non-cooperative-jurisdictions/timeline-eu-list-of-non-cooperative-jurisdictions/
[358] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000600
[359]https://www.podatki.gov.pl/media/7467/21-12-21-obja%C5%9Bnienia-art-11o-ust-1a-i-1b-na-ponowne-konsultacje-zewn%C4%99trzne.pdf
[360] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019IP0240

changes in the EU and national tax systems The document also draws attention to the fact that current tax systems and accounting methods are not prepared for the new economic, social and technological challenges of the 21st century. Major threats were also noted in the EU tax systems, including tax evasion and tax avoidance. The report also pointed out the differences between tax evasion and tax avoidance. The EU recalled that the fight against tax evasion and fraud tackles illegal acts, whereas the fight against tax avoidance addresses situations that exploit loopholes in the law or are *a priori* within the limits of the law – unless deemed illegal by the tax or, ultimately, the judicial authorities.

751. It should be noted that improving tax collection in EU countries is likely to reduce crime associated with tax evasion and the money laundering that follows it.

752. Tax havens and financial havens are known for aggressive tax planning. Aggressive tax planning is understood as the setting of a tax design aimed at reducing tax liability by using the technicalities of a tax system or arbitrating between two or more tax systems.

753. On 7 October 2022, the Sejm of the Republic of Poland adopted the *Act amending the Corporate Income Tax Act and certain other acts* (Journal of Laws of 2023, item 1059) that changes, among other things, the obligations of taxpayers in reporting haven transactions. The amending Act introduces the following amendments to the regulations: increasing the documentation thresholds (materiality thresholds) for direct haven transactions whose exceeding triggers the documentation obligation, and repealing in entirety the provisions regarding indirect haven transactions.

754. The indicated changes concerned an increase in the thresholds for preparing local transfer pricing documentation for taxpayers and companies that are not legal entities transacting directly with an entity having its place of residence, registered office or management in a territory or country applying harmful tax competition (haven entity). Currently, in accordance with the amended content of Article 11k(2a) and Article 11o(1), this threshold is changed to: PLN 2,500,000 – for financial transactions, PLN 500,000 – for transactions other than financial transactions.

Physical cross-border transportation of assets and cash transactions

755. On 3 June 2021, *Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005* began to apply in the European Union. The aforementioned Regulation of 23 October 2018 takes into account and defines a system of rules that are intended to facilitate the prevention, detection and prosecution of criminal activities as defined in *Directive (EU) 2015/849*[361] *of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*.

756. Regulation (EU) 2018/1672 imposes an obligation to submit a declaration regarding cash carried by a natural person. In accordance with the information contained in Article 3(1) of this Regulation, naturals persons carrying cash of EUR 10,000 or more shall declare that cash to the competent authorities of the Member State through which they are entering or

[361] 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

leaving the Union and make it available to them for control. The declaration shall provide details about the following: (a) the carrier, (b) the owner of the cash (natural person or legal person), (c) the intended recipient of the cash (natural person or legal person), (d) the nature and the amount or value of the cash, (e) the economic provenance of the cash, (f) the intended use of the cash, (g) the transport route, (h) the means of transport. The details described above shall be transferred to control authorities using the cash declaration form (in writing or electronically).

757. In order to prevent money laundering and terrorism financing, the obligation to submit a cash declaration has been imposed on natural persons entering or leaving the territory of the Union. This obligation at EU borders applies to those carrying cash on their person, in their luggage or in the means of transport in which they cross external borders. Such persons are required to make the cash available to the competent authorities for control and, if necessary, to present it to those authorities. The definition of 'carrier" (indicated in recital 17 of Regulation No 2018/1672) does not include those cash carriers who transport goods or persons on a professional basis.

758. The information obtained by the control authorities (registered in declarations) is then, in accordance with Article 9(1) of this Regulation, transmitted to the FIU of the Member State concerned. EU Member States shall also ensure that the FIU of a given Member State exchanges such information with the relevant FIUs of other Member States (Article 53 of *Directive (EU) 2015/849*). Moreover, Where there are indications that the cash is related to criminal activity which could adversely affect the financial interests of the Union, such information shall be transmitted by the competent authorities of each Member State to the European Commission, the European Public Prosecutor's Office or EUROPOL – in accordance with Article 10(2) of Regulation (EU) 2018/1672. Moreover, in accordance with Article 11(1) of the above Regulation, Member States or the European Commission may, within the framework of mutual administrative assistance, transmit relevant information collected by the authorities of EU Member States to third countries.

759. This information shall be transmitted to the FIU of the Member State concerned, that should ensure that the FIU, on its own initiative or upon request, transmits all relevant information to the FIUs of the other Member States. In order to ensure the effective flow of information, all FIUs shall use the EU Cash Information System (CIS) established by Council Regulation (EC) No 515/97 of 13 March 1997.

760. Under Regulation (EU) 2018/1672, the definition of cash covers four categories: currency, bearer-negotiable instruments, commodities used as highly-liquid stores of value and certain types of prepaid cards.

761. Negotiable-bearer instruments entitle their holders to claim a financial amount upon presentation of the instruments without having to prove their identity or entitlement to that amount. They can be easily used to transfer significant amounts of value and are very similar to currency in terms of liquidity, anonymity and fraud risk.

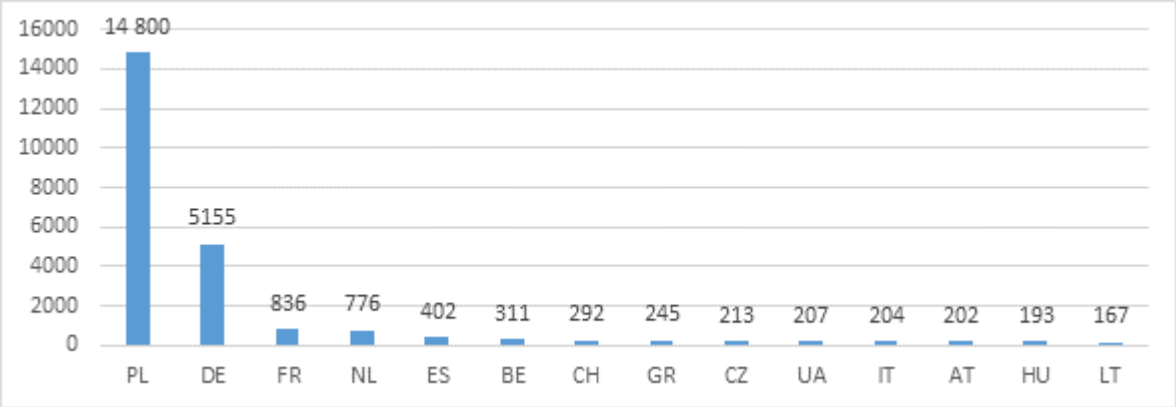
762. Commodities used as highly-liquid stores of value presents a high ratio between their value and their volume and can easily be converted into currency through accessible trading markets while incurring only modest transaction costs. Such commodities are usually presented in a standardised manner, enabling quick verification of their value.

763. Prepaid cards are non-nominal cards that store or provide access to monetary value or funds that can be used for payment transactions, for acquiring goods or services or for the redemption of currency. They are not linked to a bank account. Prepaid cards include anonymous prepaid cards as referred to in *Directive (EU) 2015/849*. They have a wide range of applications for a variety of lawful purposes, and some of these instruments also serve public interests. Such prepaid cards are easy to carry and can be used to transfer significant value across external borders.

764. In 2021-2022, the GIFI obtained through the CIS[362] information on 25,165 notifications regarding declarations of cash entering the EU and 7,368 notifications regarding declarations of cash leaving the EU.

765. Persons declaring *cash entering* the EU (in 2021-2022) provided information on the country to which they were carrying the funds. According to the data from the CIS, most declarations regarding cash entering the EU were sent to Poland (PL) – 14,800 declarations, followed by Germany (DE) – 5,155, France (FR) – 836, and the Kingdom of the Netherlands (NL) – 776 (Chart 25 below).

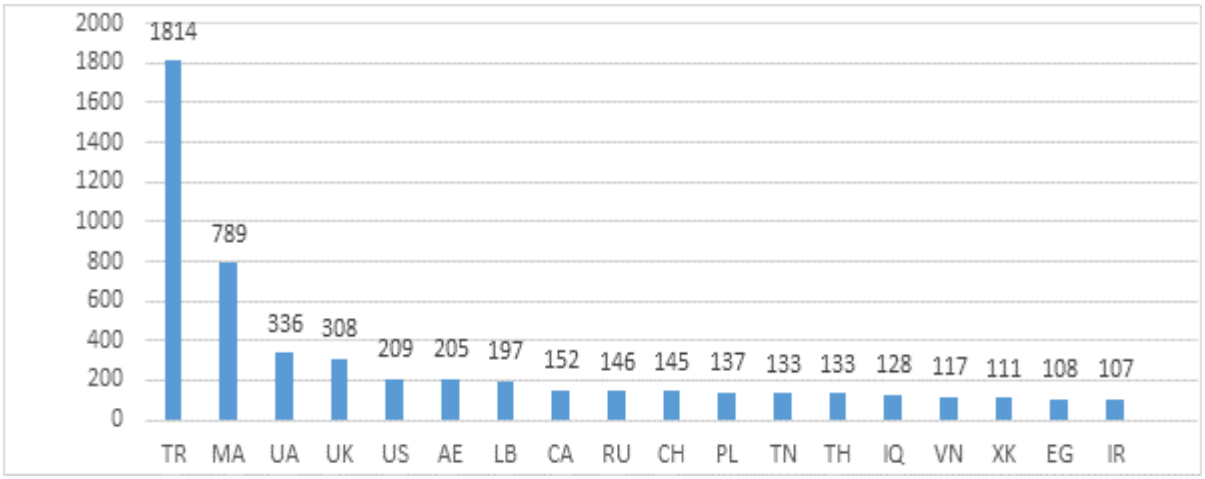
Chart 25. Countries where cash was entered into the EU in 2021-2022 (destination countries – by code[363]) by the number of submitted declarations of cash entering the EU (destination countries with more than 100 declarations submitted)



766. Based on the declaration of *cash leaving* the EU, it was established that the countries to which people most often carried cash included Türkiye, Morocco and Ukraine (Chart 26 below):

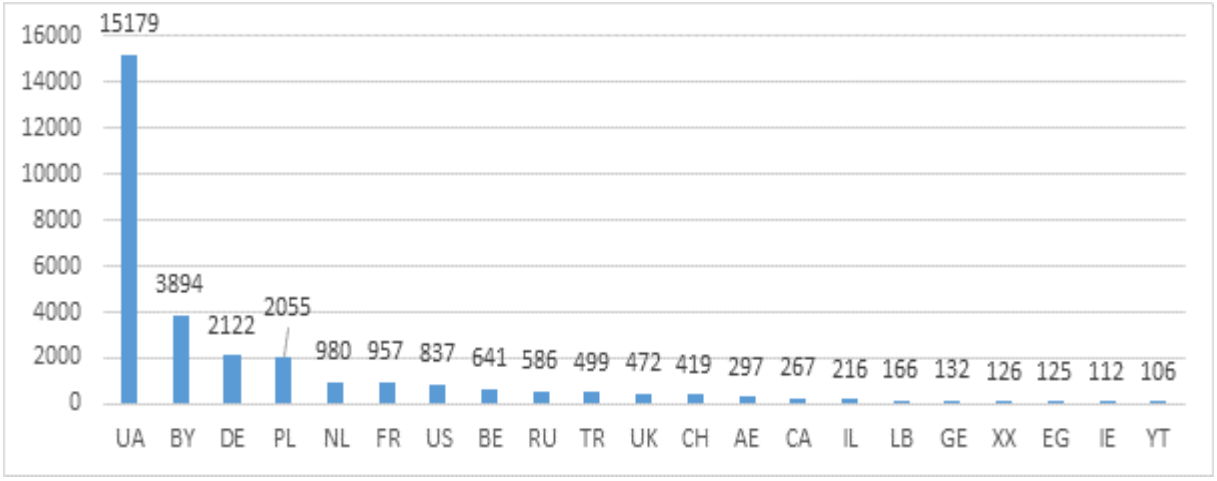
[362] UE Cash Information System. Data to be included in the CIS database regarding declarations of import and export of funds is supplemented by Polish and foreign EU customs authorities as part of the CIS functionality.
[363] https://www.panstwaswiata.pl/lista-kodow-panstw-iso-3166-1/

Chart 26. Countries from which cash was leaving the EU in 2021-2022 (destination countries – by code[364]) by the number of submitted declarations of cash leaving the EU (destination countries with more than 100 declarations submitted)



767. Based on declarations of *cash entering* the EU in 2021-2022, it was determined that the greatest numbers of declarations of cash entering the EU (the country from which the cash left the EU) came from Ukraine (UA) – 15,179 declarations, Belarus (BY) – 3,894 declarations, Germany (DE) – 2,122 declarations, and Poland (PL) – 2,055 declarations.

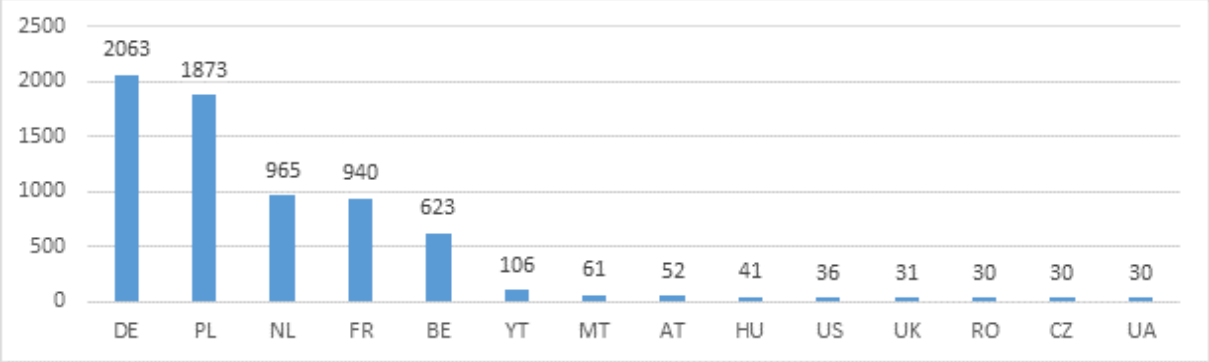
Chart 27. Countries from which cash left the EU in 2021-2022 (countries by code) by the number of submitted declarations of cash entering the EU[365]



[364] Ibidem
[365] countries with more than 100 submitted declarations

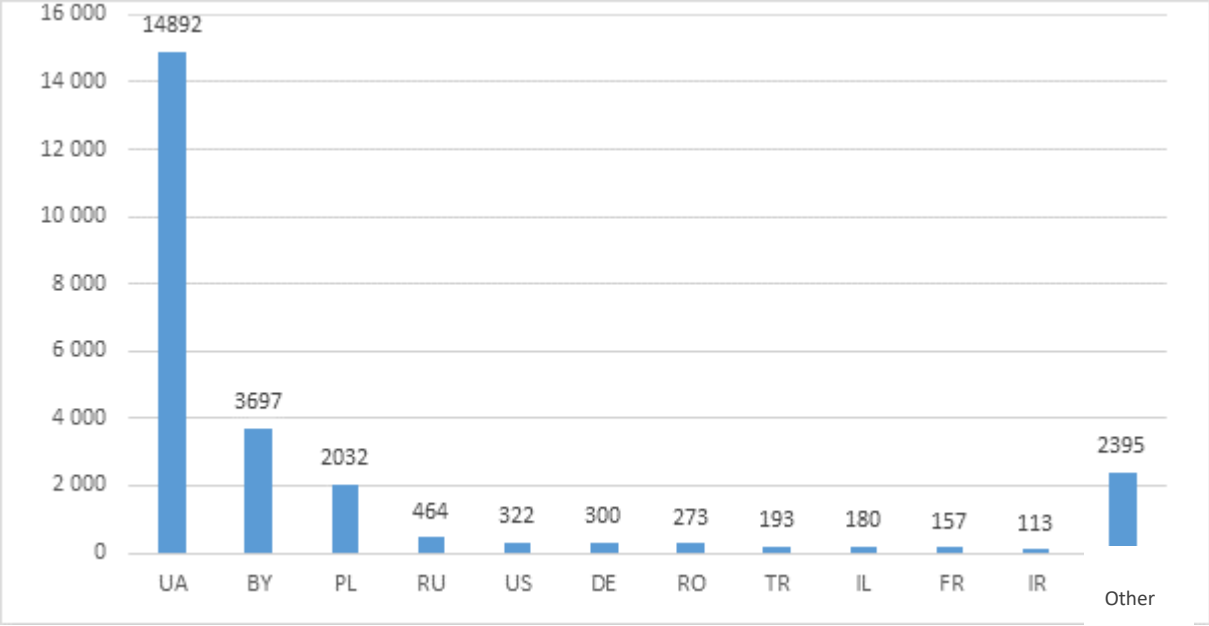
768. Based on declarations of *cash leaving* the EU in 2021-2022, it was determined that the greatest numbers of declarations of cash leaving the EU (the country from which the cash left the EU) came from Germany (DE) – 2,063 declarations, Poland (PL) – 1,873 declarations, Kingdom of the Netherlands (NL) – 965 declarations, and France (FR) – 940 declarations.

Chart 28. Countries from which cash left the EU in 2021-2022 (countries by code) by the number of submitted declarations of cash leaving the EU[366]



769. As regards information regarding the citizenship of persons that declared cash entering the EU in 2021-2022, the greatest numbers of declarations were submitted by citizens of Ukraine (UA) – 14,892 persons, Belarus (BY) – 3,697 persons, Poland (PL) – 2 032 persons, and Russia (RU) – 464 people. See: Chart 29 below.

Chart 29. Information regarding the citizenship of persons that declared cash entered into the EU in 2021-2022

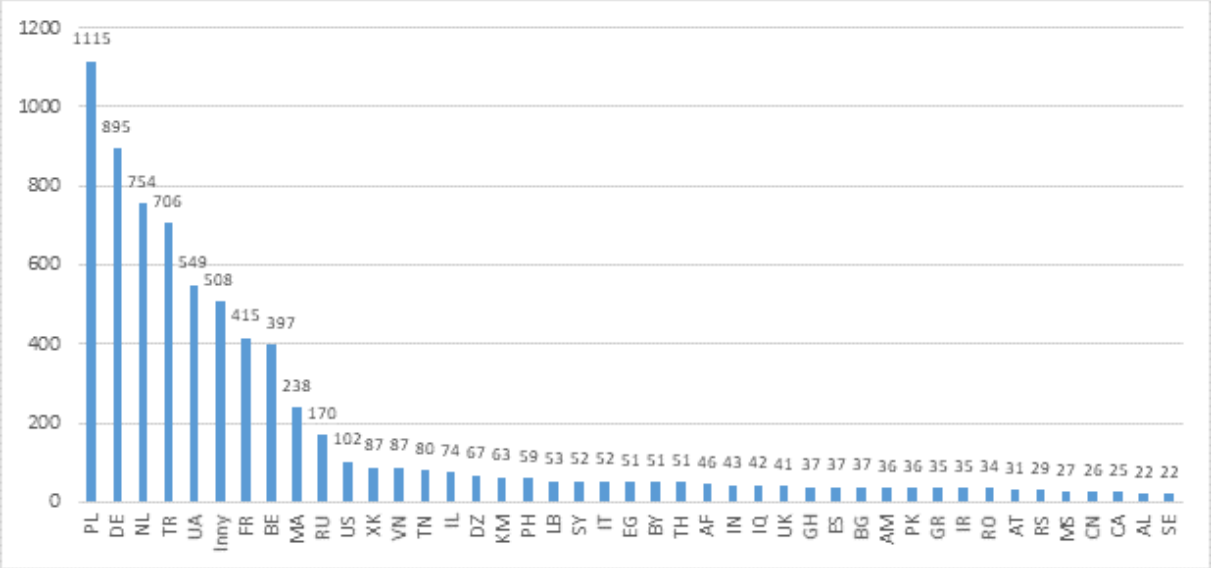


770. As regards information regarding the citizenship of persons that declared *cash leaving the EU* in 2021-2022, the greatest numbers of declarations were submitted by citizens of Poland

[366] countries with at least 30 submitted declarations

(PL) – 1,115 persons, Germany (DE) – 895 persons, the Kingdom of the Netherlands (NL) – 754 persons, and Türkiye (TR) – 706 persons. See: Chart 30 below.

Chart 30. Information regarding the citizenship of persons that declared cash leaving the EU in 2021-2022



771. Based on declarations of *cash entering the EU* submitted in 2021-2022, its total value in this period was EUR 1,803,171,506.02[367] (see: Table 29 and Chart 31 below). The largest amounts of cash were brought into the EU by citizens of Ukraine – EUR 1,227,987,493.86 (68.10%), Poland – EUR 188,789,931.89 (10.47%), and Belarus – EUR 144,979,189.72 (8.04%). In the case of Ukraine, the greatest amount of cash *brought into the EU* by its citizen is due to their migration caused by the ongoing war in that country.

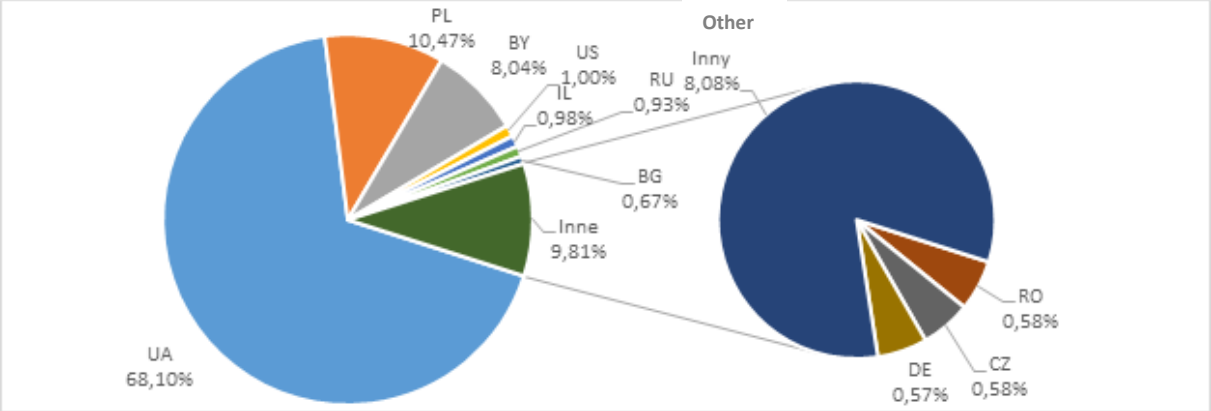
Table 29. Value of declared cash entering the EU (in EUR) by citizenship

Citizenship	Value of declared cash entering the EU (in EUR)
UA – Ukraine	1,227,987,493.86
PL – Poland	188,789,931.89
BY – Belarus	144,979,189.72
US – United States	18,064,440.46
IL – Israel	17,689,369.27
RU – Russia	16,707,734.27
BG – Bulgaria	12,045,799.35
RO – Romania	10,505,707.08
CZ – Czech Republic	10,391,231.82
DE – Germany	10,308,187.49

[367] Value in EUR calculated at the average NBP exchange rates based on information on the declared currencies

Other	145,702,420.81
Total	**1,803,171,506.02**

Table 31. *Value of declared cash entering the EU (in EUR) by citizenship (in percent)*



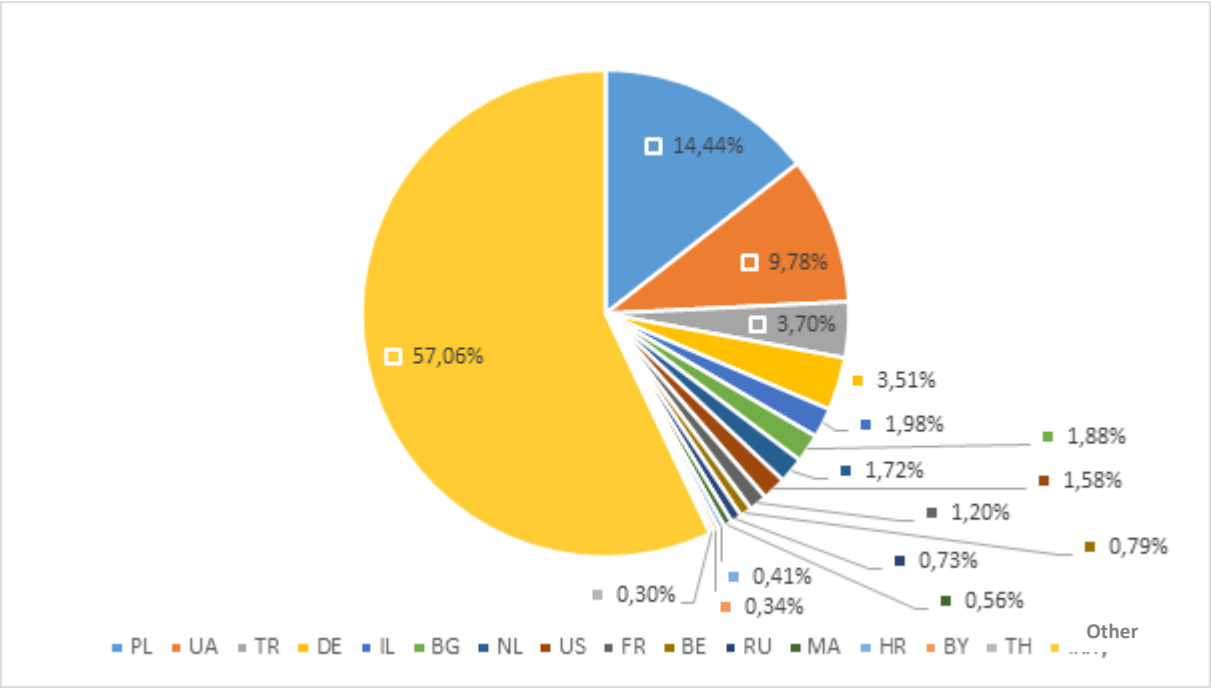
772. Based on declarations of cash leaving the EU submitted in 2021-2022, its total value in this period was EUR 678,626,491.97[368] (see Table 30 and Chart 32 below).

Table 30. Value of declared cash leaving the EU (in EUR) by citizenship

Citizenship	**Value of declared cash leaving the EU (in EUR)**
PL – Poland	98,023,879.43
UA – Ukraine	66,370,832.12
TR – Türkiye	25,103,211.67
DE – Germany	23,817,378.07
IL – Israel	13,455,156.64
BG – Bulgaria	12,746,470.59
NL—Kingdom of the Netherlands	11,669,740.07
US – United States	10,752,731.59
FR – France	8,169,767.03
BE – Belgium	5,387,618.14
RO – Romania	4,967,304.13
MA – Morocco	3,829,352.11
HR – Hungary	2,754,510.26
BY – Belarus	2,289,239.29
TH – Thailand	2,035,512.66
Other	387,253,788.18
Total	**678,626,491.97**

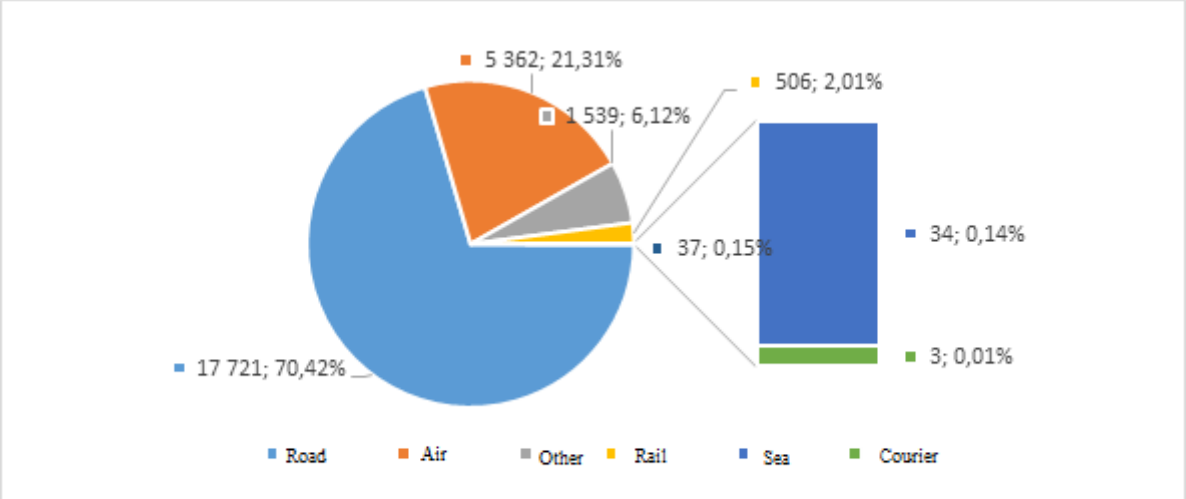
[368] Ibidem

Chart 32. Value of declared cash leaving the EU (in EUR) by citizenship (in percent)



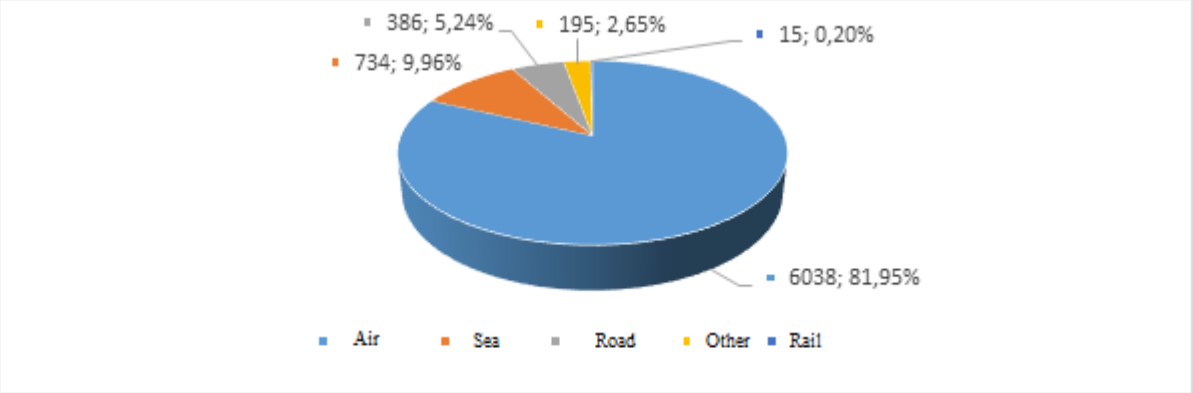
773. The information contained in the declarations of cash entering the EU also recorded the type of transport used to carry it. In the declarations of cash entering the EU, it was brought into the EU by road, air, rail, sea, courier and using other forms of transport. According to Chart 33 below, the greatest amounts of cash entered the EU by road (over 70% of the submitted declarations) and by air (over 21% of the submitted declarations).

Chart 33. Information on the type of transport used in the case of cash entering the EU



774. In turn, in the case of the submitted declarations of cash leaving the EU, the greatest amounts of cash left the EU using air transport (almost 82% of the submitted declarations) and sea transport (almost 10% of the submitted declarations). In the case of road transport, over 5.2% of declarations of cash leaving the EU were submitted – see Chart 34 below.

Chart 34. Information on the type of transport used in the case of cash leaving the EU



Real estate trade

775. The real estate sector is one of the areas used by criminal organisations to launder illicit funds. This sector has many features that make it attractive for money laundering and terrorism financing. The real estate market is generally international in nature, geographically divided, and there are numerous factors that determine the local real estate price. The price of real estate in a given location and at a given time is affected by a number of factors that underlie the correct valuation of a given real estate market. Money laundering transactions carried out on a given real estate market can be easily disguised as real commercial transactions among the huge number of real estate transactions. What affects the degree of complexity of detecting suspicious transactions on this market is often – especially in countries defined as developing markets – a lack of relevant information (e.g. statistical data on the average market price of real estate) that could constitute a reference point for determining whether real estate purchase transactions economically viable.

776. Suspicious transactions on the real estate market may also have undesirable political effects, contributing to the institutional and economic destabilisation of specific countries. Due to the international nature of the real estate market, it is often very difficult to distinguish real estate transactions from those related to money laundering or terrorism financing. The inflow of funds to a specific country causing changes in real estate prices may have a significant impact on investment decisions made by potential real estate buyers and sellers. They also influence the investment decisions of state and local government bodies. Real estate prices can also have a significant impact on the construction industry, determining its development or stagnation. All these factors together suggest that price changes occurring on the real estate market, as well as the development or stagnation of the construction industry, significantly affect the economic activity and development of a given country.

777. There are many methods, techniques, mechanisms and instruments that make it possible to use the real estate sector for money laundering and terrorism financing. Most of these methods are illegal per se, but some may be considered completely legal if they were not used with the intention of laundering money or financing of terrorism (or if this link could not be detected). There is also great diversity in the possible types of transactions that may be linked to money laundering or terrorism financing on the real estate sector. However, this does not mean that all transactions that do not seem sufficiently economically viable are necessarily

related to illegal activities resulting in money laundering or terrorism financing. It should be remembered that money laundering always seeks to disguise itself as a "normal" transaction. The criminal nature of activities on the real estate market results from the origin of the funds used and the intentions of the transaction participants.

778. The aspects of the risks occurring on the real estate market are addressed in the FATF report from July 2022 – "Guidance for a risk-based approach – Real estate sector"[369]. The document refers to numerous aspects related to money laundering and terrorism financing on the real estate market, i.e. it analyses threats, contains good practice and indicates vulnerabilities to risks directly related to the real estate market. It also provides instructions for entities supervising this market (guidance that reduces the risk of money laundering and terrorism financing).

779. A number of common features can be identified in real estate transactions that, when detected individually or in combination, may indicate the potential use of the real estate sector for the purposes of money laundering and terrorism financing. Often, the real estate transaction itself seems legal, but some of the subjective or objective factors involved may indicate links to money laundering or terrorism financing. The criminal nature of these transactions results from the origin of the funds and the purpose for which these transactions are carried out by their participants. The basic factors increasing the risk of money laundering or terrorism financing on the real estate market include:

- persons residing or entities based in high-risk countries (e.g. tax havens) taking part in the transaction,
- persons or companies that, based on the analysis performed, seem to lack the economic capacity to enter into a transaction on the real estate market, or the transaction amount disproportionate to the assets reported by the transaction participant,
- transactions carried out by persons related (directly or indirectly) to criminal activities,
- transactions involving persons with business, family or social links,
- transactions involving quick repayment of a large loan or mortgage – especially where the repayment is made in cash,
- transactions where there is no connection between the transaction and the activities conducted by the purchasing company or where the company does not conduct business activities,
- transactions that do not seem economically viable or where one of the parties incurs an obvious loss,
- transactions where, based on the analysis performed, there are grounds for assuming that the parties thereto are not acting on their own behalf, but are trying to hide the identity of the actual customer;

[369] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-real-estate-sector.html

- transactions where payments are made in cash or other negotiable instruments that do not identify the actual payer,
- transactions where the legal tenders used to conclude the transaction come from high-risk countries,
- transactions where the purchase of real estate and its sale take place within a short time and that result in a significant increase or decrease in the price compared to the purchase price,
- transactions where the price is much different (much higher or much lower) than the actual value of the real estate or much different from market prices.

780. According to the report published by Statistics Poland in November 2022 entitled *"Obrót nieruchomościami w 2021 r.*" (Real estate trade in 2021)[370] prepared using notarial reporting conducted by the Ministry of Justice, 701.5 thousand notarial deeds regarding the sale of real estate were signed in Poland in 2021, i.e. 24.3% more than a year earlier. The highest increase was recorded in the number of notarial deeds regarding the sale of undeveloped plots (by 33.3%) and the sale of residential premises (by 22.9%) as well as the granting of perpetual usufruct by the State Treasury or local government units along with the sale of buildings (by 22.9%) In the structure of notarial deeds regarding the sale of real estate in 2021, the sale of residential premises prevailed and accounted for 36.7%. Sales of undeveloped plots (26.9%), sales of agricultural property (10.9%), sales of plots with residential buildings (10.4%), and sales of cooperative ownership rights to premises (7.3%) also accounted for a significant percentage of real estate traded. In 2021, prices of residential premises were 9.2% higher than a year before (in 2020 – by 10.5%). Price increases occurred both on the primary and secondary markets (by 9.1% and 9.3%, respectively).

781. Besides the aforementioned report published by Statistics Poland, the National Bank of Poland also publishes quarterly reports regarding information on housing prices and the 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 that occur on the residential and commercial real estate market in largest cities in Poland[371]. The NBP also prepares annual reports[372], providing economic operators, including real estate market participants, with the most complete, reliable and objective information on 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 report presents more detailed information broken down by the sixteen markets in the capitals of Poland's voivodeships.

782. The NBP also publishes a database of residential real estate prices[373] that includes both offer and transaction prices for the sale and rental of flats within the administrative borders of

[370]https://stat.gov.pl/obszary-tematyczne/infrastruktura-komunalna-nieruchomosci/nieruchomosci-budynki-infrastruktura-komunalna/obrot-nieruchomosciami-w-2021-roku,4,19.html, read on 14.01.2023
[371] https://nbp.pl/publikacje/cykliczne-materialy-analityczne-nbp/rynek-nieruchomosci/, read on 14.01.2023
[372] https://www.nbp.pl/home.aspx?f=/publikacje/rynek_nieruchomosci/index1.html, read on 14.01.2023
[373] https://www.nbp.pl/home.aspx?f=/publikacje/rynek_nieruchomosci/index2.html, read on 14.01.2023

16 voivodeship capitals and Gdynia where a significant percentage of real estate turnover takes place (prices include VAT).

783. An analysis of transaction prices and forecasts for the residential real estate market in Poland called E-VALUER INDEX is prepared annually by Emmerson Evaluation Sp. z o.o. According to the report for H1 2022[374], low interest rates, low interest rates on savings products as well as rising inflation in 2020-2021 encouraged Poles to invest their capital in real estate. The beginning of 2022 saw a considerable deterioration in buyers' sentiment caused by regular increases in interest rates by the Monetary Policy Council. In September, the reference rate reached 6.75%, i.e. the highest level since 2002. The limited availability of loans and a significant increase in instalments discouraged some potential buyers. Investors adopted a wait-and-see attitude, began to closely monitor the market situation and analyse the then-current opportunities. The real estate market is also affected by the conflict between Russia and Ukraine that turned into permanent hostilities. The costs of newly constructed buildings increased due to the outflow of Ukrainian workers (mainly men) returning to their country to defend their homeland. The prices of fuel, energy and other raw materials also increased, leading to further increases in the prices of construction materials, whose limited availability was yet another problem. The war had an impact on supply chains as well as production itself. Ukraine is a major producer of steel – widely used in construction. On the other hand, Russia's aggression against Ukraine significantly affected the demand on the flat rental market (due to refugees seeking residential premises to rent). Mass migration from the East, especially in the initial phase of the conflict, resulted in the limited availability of premises for rent and, as a result, increased rental prices. In the first half of 2022, the number of new flats put into use by developers was 6% lower than in the first half of 2021.

784. Given the relatively high percentage of cash transactions on the real estate market in Poland, important information for the AML/CFT purposes in real estate trade may be provided by entities involved in real estate transactions that match the parties to these transactions, namely real estate brokers. Real estate brokerage itself involves paid activities aimed at concluding contracts by other people, but due to the different scope of concluded brokerage contracts, the broker's knowledge of the details of the transaction may be very extensive. Due to the fact that the provision of real estate brokerage services is not a licenced profession and requires only civil liability insurance, there is no precise information on the number of real estate brokers in Poland. As at 14 January 2023, the Central Register of Real Estate Managers and Real Estate Brokers maintained by the National Chamber of Real Estate Management (KIGN) [375] listed 3,792 entities, but there is also the National Register of Real Estate Brokers[376] run by the Polish Real Estate Federation (FPPRN) (available by telephone or email). Real estate brokers are obligated institutions within the meaning of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*.

[374] https://www.emmerson-evaluation.pl/czytaj-nasze-publikacje/, read on 14.01.2023
[375] http://www.kign.pl/rejestr/, read on 14.01.2023
[376] https://pprn.pl/?page_id=13612, read on 14.01.2023

785. Besides real estate brokers, transactions concluded on the real estate market also involve representatives of legal professions.[377] The Polish National Council of Notaries operates the Notarial Registers IT system that includes: the Inheritance Register, the Notarial Register of Wills (NORT), the Central Repository of Electronic Copies of Notarial Deeds (CREWAN), the Register of Succession Administrators, the Register of Users, and Notarial Statistical Registers.

786. The acquisition by a foreigner of the ownership right or the right of perpetual usufruct of real estate as well as the acquisition of or subscription for shares in commercial companies based in the territory of Poland that are owners or perpetual usufructuaries of real estate located in Poland by a foreigner requires the authorisation of the minister competent for the interior. In order to obtain such authorisation, a foreigner should apply for it. The acquisition of real estate and shares in companies being owners or perpetual usufructuaries of real estate located in Poland by foreigners from the European Economic Area and the Swiss Confederation does not require the authorisation of the minister competent for the interior.

Crowdfunding

787. On 29 July 2022, the provisions of the *Act of 7 July 2022 on crowdfunding for business and assistance to borrowers* (Journal of Laws of 2023, item 414) entered into force. This is the first legal act in Poland that formally regulates crowdfunding and the activities of crowdfunding platforms.

788. Crowdfunding is defined in Article 2(16) of the aforementioned Act, according to which a crowdfunding service is defined in Article 2(1)(a) of *Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937*. It should also be noted that there are many definitions of crowdfunding and with varying degrees of detail. These contain, however, common elements through which it is possible to determine what is meant by this concept: the investors' support is always of a financial nature, the fundraiser is carried out via the Internet, the investors receive various rewards in return for their payments, the fundraising campaign is usually carried out for a specific time, the funding campaign is open at two levels, i.e. anyone can make a donation from anywhere and in any amount, it is known who is raising money, for what purpose and what amount of money is to be ultimately raised.

789. Crowdfunding is an increasingly popular way for companies to obtain funding. The rapid development of this type of funding also translates into subsequent legislative changes and novelties. The new regulations apply to investment-based crowdfunding and lending-based crowdfunding. *The Act on crowdfunding for business and assistance to borrowers* complements

[377] Pursuant to Article 2(1)(13), (13a) and (14) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the list of obligated institutions includes notaries – in so far as they perform activities in the form of a notarial deed, including:

- transfer of the ownership of an asset, including the sale, exchange or donation of movable property or real estate,
- conclusion of an agreement on the division of inheritance, dissolution of co-ownership, life annuity, pension in exchange for the transfer of the ownership of real estate and on the distribution of jointly held assets,
- assignment of the cooperative member's ownership right to premises, perpetual usufruct right, and the alleged promise of separate ownership of premises, as well as attorneys, legal counsels, foreign lawyers, tax advisors in so far as they provide the client with legal assistance or tax advisory services regarding the purchase or sale of real estate, an enterprise or an organised part of an enterprise.

the regulations on crowdfunding contained in *Regulation (EU) 2020/1503 of the European Parliament and of the Council on European crowdfunding service providers for business*[378].

790. Crowdfunding is an increasingly recognised form of alternative funding for start-ups and small and medium-sized enterprises, and is usually based on small investments. Crowdfunding represents an increasingly important type of intermediation where a crowdfunding service provider, without taking on own risk, operates a digital platform open to the public in order to match or facilitate the matching of prospective investors or lenders with businesses that seek funding. Such funding could take the form of loans or the acquisition of transferable securities or of other admitted instruments for crowdfunding purposes.

791. In its 2022 report on the supranational assessment of the risk of money laundering and terrorist financing in the EU, the European Commission drew attention to crowdfunding[379]. In this document, the EC draws attention to the fact that crowdfunding may be used to finance terrorism by using crowdfunding platforms that are made available on the Internet. It indicated, among others, that funds may be raised in this way for fictitious purposes and transferred abroad for money laundering or terrorism financing. This threat is also mentioned by the European Banking Authority (EBA) in its report of March 2021.[380]

792. The EC notes that from 10 November 2023, *Regulation of the European Parliament and of the Council on European crowdfunding service providers for business*[381] will be in force, that will require all payments to be made via an authorised payment service provider and certain measures to mitigate crowdfunding risks to be introduced. Pursuant to the above Regulation, in order to carry out crowdfunding activities the entity must be entered in the register of crowdfunding platforms kept by the European Securities and Markets Authority[382]. The said register should include information on all operating crowdfunding platforms in the Union. Entities that no longer meet the rules related to their authorisation on this list would be deregistered[383]. Moreover, crowdfunding platforms, depending on the activities carried out, must ensure protection of investors adequate to their type, i.e.: sophisticated investor or non-sophisticated investor[384].

793. Crowdfunding can take many forms, such as:

- donation-based crowdfunding – raising funds for a specific purpose with no return benefit from the project owner/beneficiary,

[378] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32020R1503
[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 activities, European Commission, Brussels, 27.10.2022, pp. 52-56, at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0344
[380] EBA report on money laundering and terrorist financing risk affecting the EU financial sector of 3 March 2021, p. 22.
[381] REGULATION (EU) 2020/1503 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1503
[382]https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/esma_pl
[383] Ibidem, p. 6
[384] Ibidem, p. 6

- reward-based crowdfunding – in return for donating funds, investors receive a specific type of gratification, that, however, does not necessarily have to be the economic equivalent of the donated funds,
- crowdfunding based on pre-sales – investors donate funds to create a product that is delivered to them by the beneficiary after some time,
- equity crowdfunding – individuals invest in the beneficiary's venture in exchange for a stake in its company,
- debt crowdfunding – the investors' contribution is repayable, i.e. the beneficiary undertakes to return the funds received.

794. According to the EC report on crowdfunding in the EU, the following types of crowdfunding can also be distinguished:

- invoice trading crowdfunding – the beneficiary transfers unpaid invoices or receivables (individually or in a bundle) to investors in exchange for their funds,
- hybrid model of crowdfunding – a model combining elements of various types of crowdfunding.

795. According to the report entitled *"Polskie Startupy 2021"*[385] (Polish Startups 2021) developed by Startup Poland, crowdfunding and crowdinvesting accounted for 4% of the startup funding sources in Poland.

796. Recently, starting from 2019, investment crowdfunding, i.e. an alternative way of raising capital, has been increasingly popular. According to information available on the website of the Office of the Polish Financial Supervision Authority[386], investment crowdfunding should not be treated as competition for the stock exchange, but as part of the evolving capital market. It should be perceived as the first step on the way to an IPO on the Warsaw Stock Exchange. It is also often the case that individual investors support companies at the earliest stages of their development, while professional investors (venture capital/private equity funds) enter the company only in later rounds.

797. Investment crowdfunding is based on crowdfunding platforms that are used to conduct activities where those providing capital have investment goals. In this crowdfunding model, capital is obtained, among others, through the issue of securities or shares in limited liability companies.
Depending on the functionality of a given platform, the activities conducted through it may require its operator to hold an authorisation to conduct brokerage activities, or may be within the limits of freedom of business activity[387].

798. Crowdfunding enables raising the necessary capital quickly and easily, without having to fulfil the obligations related to, for example, obtaining a loan from credit and financial institutions or offering company shares in a traditional public offering, or time-consuming searching for funding among venture capital funds. According to the Polish Agency for Enterprise Development (PARP), this funding method is mainly used by small and medium-

[385] https://startuppoland.org/raporty/
[386] https://www.knf.gov.pl/dla_rynku/crowdfunding_inwestycyjny
[387] https://www.knf.gov.pl/dla_rynku/crowdfunding/platformy

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".[388]

799. Some crowdfunding platforms also offer other services, such as developing customer ideas using the 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, prospectus, legal services after a successful issue or handling the shipment of shares).

800. The threat of using crowdfunding for money laundering results primarily from its attributes, such as the extensive anonymity of individuals and entities providing funds to the beneficiary and the possibility of making international investments.

801. Currently, crowdfunding platforms are not obligated institutions under the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, unless – in connection with the provision of additional services by them (e.g. payment services, currency exchange or the services referred to in referred to in Article 2(1)(16) of the aforementioned Act) they fall under the provisions of the aforementioned normative act. Therefore, they are not obliged to apply customer due diligence measures or to provide the GIFI *ex officio* and upon request with the information specified in the aforementioned Act.

802. It should also be noted that the *Act of 7 July 2022 on crowdfunding for business and assistance to borrowers*:

- indicates the Office of the Polish Financial Supervision Authority as the authority competent to supervise providers of crowdfunding services for business, and grants it relevant supervisory powers (among others, to suspend specific crowdfunding offers or suspend the activities of suppliers as well as to cooperate with judicial authorities and supervisory authorities from other EU Member States),
- introduces adequate administrative and criminal sanctions for non-compliance with the provisions of the Act.

803. While crowdfunding platforms usually identify project beneficiaries, they rarely do so in the case of investors. Moreover, sometimes forms of funding are allowed that may additionally facilitate the concealment of the details of investors (e.g. cryptocurrencies or prepaid cards[389] – issued by some foreign operators without registering their users, that are then resold by the beneficiary). International transactions are also possible via crowdfunding platforms, that may also make it difficult to identify investors that make transactions from other countries[390].

---

[388]https://www.parp.gov.pl/component/content/article/54127:crowdfunding-zasady-dzialania-i-europejskie-plany-regulacyjne

[389] COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0344

[390] "For crowdfunding campaigns to be successful, it is particularly important to reach as many interested potential investors as possible, and their nationality or place of residence are usually irrelevant. That is why international and cross-border crowdfunding campaigns are most successful, as they enable raising the greatest

804. The main threats related to the activities of crowdfunding platforms include:

- possibility of blending profits from legal and illegal sources,
- possibility of anonymous transfer of crime proceeds to third parties,
- possibility of legitimising crime proceeds by claiming that their originate from crowdfunding campaigns,
- possibility of selling crime proceeds by transferring them in return for the funds received.

Formation of business entities and their handling

805. In the Commission's report on the assessment of the risk of money laundering and terrorist financing (developed by the European Commission on 27 October 2022)[391], relatively numerous risk scenarios were identified, involving, among others, the creation of complex structures by criminal groups, very often covering various jurisdictions (in particular offshore ones), with hidden ownership connections, under which the beneficial owners of subsequent entities operating within these structures are based in countries other than those where these entities are registered.[392] Persons acting as representatives of established entities and being formally responsible for them are often only a cover for the real beneficial owners. In this way, representatives of criminal groups can remain anonymous and introduce crime proceeds into the legal economy

806. In terms of costs, setting up a business or legal arrangement is usually quite simple and, in many cases, it can be done online. Relatively greater costs or higher levels of knowledge and planning may be required where criminal organisations use intermediaries to create more complex/complicated organisational structures. Knowledge of national and international regulatory and tax laws is also useful in such situations and can often only be provided by professional intermediaries.

807. According to the FATF analysis, extensive ownership structures created to conceal beneficial owners include mainly companies that do not actually conduct business activities or any other independent operations, and do not have employees or any significant assets (shell companies). Operating companies having features typical of legal companies are also used to hide and obscure illegal financial activities (front companies), as well as stocks and bearer shares, although these forms are less popular.[393]

808. The methods used also include other options, including: – apart from "straw men", formally representing business entities – also other legal persons claimed to be directors in controlled business entities, trusts and other similar legal arrangements, as well as shell

amounts of funds in the shortest time"- https://www.parp.gov.pl/component/content/article/54127:crowdfunding-zasady-dzialania-i-europejskie-plany-regulacyjne

[391]https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en

[392] 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, 27.10.2022, pp. 138-152 (Annex 1 – Risk analysis by products), at: https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en

[393] Concealment of Beneficial Ownership, FATF, July 2018, p. 5, at: https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html.

companies (i.e. companies with inactive shareholders, directors and a secretary, that remain dormant for a long period, although relationships with clients have already been established – sometimes these companies are considered a type of shell companies) as well as intermediaries facilitating the establishment of the aforementioned business entities.[394] Typical criminal methods related to falsifying activities are also used (e.g. using false documents).

809. According to the FATF analysis carried out for the purposes of drawing up the report entitled "Concealment of Beneficial Ownership", the services of trust and company service providers were most often used out of all types of services offered by intermediaries facilitating the formation of business entities.[395]

810. According to the analytical proceedings conducted by the GIFI from January 2019 to August 2022 (especially those regarding suspected laundering of money originating from fiscal offences), the entities involved in suspicious financial flows often included business entities that were established and/or run by such intermediaries. The fact that business entities formed by such intermediaries could be used for criminal purposes was indicated, among others, by the following factors: shareholders/owners being straw men having no assets 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.

811. According to the information held by the GIFI, the shareholders/owners of some of the business entities established in the territory of the Republic of Poland include foreigners. The *Act of 6 March 2018 on the rules for participation of foreign economic operators and other foreign persons in economic transactions in the territory of the Republic of Poland* (Journal of Laws of 2022, item 470) indicates which foreigners can conduct business activity in Poland on the same terms and conditions as Polish economic operators and which of them are subject to certain restrictions in this respect. Article 4(1) of the aforementioned *Act* provides that foreign persons from EU Member States may undertake and conduct business activities in the territory of the Republic of Poland on the same terms and conditions as Polish citizens. In accordance with Article 4(2) of the aforementioned *Act*, foreign persons who are not citizens of any EU country must meet certain conditions (listed in that *Act*) to be able to conduct business activity in the territory of the Republic of Poland.

812. Attention should also be paid to the frequency of using limited liability companies in criminal activities. According to the GIFI's experience, business entities operating in the form of limited liability companies are more susceptible to abuse, e.g. by organised criminal groups, including international ones.

813. According to Statistics Poland data, as at the end of 2022[396], there were 539,811 limited liability companies established in Poland, accounting for approx. 10.8% of all types of companies established in that year. At the same time, a steady increase in the number of new business entities in the form of limited liability companies should be noted, whose numbers in 2020 and 2021 were 4,663,378 and 4,836,214, respectively.

[394] Ibidem, pp. 25-45.
[395] Ibidem, p. 6.
[396] https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/zmiany-strukturalne-grup-podmiotow-gospodarki-narodowej-w-rejestrze-regon-2022-r-,1,27.html,

814. Business entities that may generate increased AML/CFT risk include simple joint-stock companies that were introduced into the *Code of Commercial Partnerships and Companies* on 1 July 2021. The entry into force of a simple joint-stock company structure means that it now one of the obligated institutions listed in the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. In the case of a simple joint-stock company, the following beneficial owners are possible: a natural person conducting business activity, a partner in a partnership or a person who is a shareholder of this company and who is entitled to ownership of more than 25 percent of the total number of shares of this legal person. Moreover, it should be noted that in the case of a simple joint-stock company, certain requirements do not apply, including that to have a minimum share capital or to pay tax on civil law transactions in certain situations (simple joint-stock companies are entitled to exemption from this tax in certain cases).

815. Information regarding natural persons and entities covered by the GIFI's notifications addressed to prosecutors' offices from January 2019 to August 2022 is presented below.

Table 31. Natural persons and natural persons conducting business activity (country-abbreviation) – their estimated percentage[397] in the GIFI's notifications sent to prosecutors' offices (selected percentage values)

Natural persons[398]		Natural persons conducting business activities[399]	
PL	35.00%	PL	4.10%
UA	9.44%	n.d.	3.73%
n.d.[400]	8.33%	UA	0.41%
IT	3.57%	VN	0.21%
LV	3.41%	RU	0.08%
VN	2.91%	DE	0.08%
IN	2.63%	SE	0.08%
HU	2.42%	BY	0.08%
FR	2.30%	RO	0.08%
RO	1.60%	LV	0.08%
RU	1.40%	IT	0.08%
BE	1.27%	EE	0.04%
BY	1.23%	UZ	0.04%
DE	1.23%	BG	0.04%
NL	1.19%	FR	0.04%

[397] for the period from 1 January 2019 to 23 August 2022
[398] selected percentage values: for natural persons – percentage value over 1%
[399] selected percentage values: for natural persons running business activity – percentage value over 0.04%
[400] no data/information on the citizenship held by a given natural person/natural person conducting business activity

Table 32. Types of entities and their percentage in the total number of entities covered by the GIFI's notifications sent to prosecutors' offices [401]

Type of entity	Percentage
natural person	48.44%
limited liability company	28.78%
foreign enterprise	9.34%
natural person conducting business activity	4.59%
other (including: limited partnership, joint-stock company, limited liability company in organisation, civil partnership, general partnership, foundation, social and professional organisation, branch or representative office of a foreign enterprise operating in the territory of the Republic of Poland, limited joint-stock partnership, association, partnership).	8.85%

816. In Poland, in accordance with the *Act of 6 March 2018 – Economic Operators' Law*, the principle of freedom of business activity prevails, enabling any undertaking permitted by law. A relevant licence, permit or entry in the register of regulated activities is required only to conduct business activities in areas that are particularly important for the security of the state or citizens or other important public interest, where this activity may not be performed freely. In accordance with Polish law, an economic operator is as a natural person, a legal person or an organisational unit that is not a legal person, having legal capacity under other law, as well as a partner in a civil partnership with respect to its business activity. Business activity may be commenced on the day of filing an application for entry in the Central Register and Information on Economic Activity (CEiDG) or upon entry in the register of companies of the National Court Register, unless specific provisions provide otherwise. However, a capital company in organisation may undertake business activity before entry in the register of companies.

817. According to data from the Central Economic Information Centre, approx. 1,000 companies are established in Poland every day. In the period from November to the end of December 2022, 55,713 companies started operating[402], while in the same period of 2021, this figure was 59,622.[403]

818. Polish law provides for conducting business activity in the following forms:

- sole proprietorship,
- civil partnership,
- partnerships: general partnership, professional partnership, limited partnership, limited joint-stock partnership,
- capital companies: limited liability company and joint-stock company,
- simple joint stock companies,
- family foundation.

As regards commercial companies, limited liability companies are the most popular In cases conducted by the GIFI, this type of company accounted for 28.78% of the total number of entities covered by the GIFI's notifications in 2019-2022.

[401] for a period from 1 January 2019 to 23 August 2022
[402] https://www.coig.com.pl/nowe-firmy-w-polsce_2016_2015_2014_2013.php, read on 15.01.2023
[403] Ibidem, read on 15.01.2023

819. For several years, some types of business activities can also be registered in Poland online.[404]

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. Estimation of inherent risk

Level of threat

820. According to the methodology laid down in Annex No. 1, calculation of the level of threat of money laundering for the purposes of inherent risk assessment should be based on the estimation of the illicit proceeds, assessment of the proceeds generating crime threat to Poland, level of risk of money laundering in the EU in the supranational assessment of the risk of money laundering and financing of terrorism as well as any information on Poland deriving from the money laundering and terrorism financing risk assessment of the other states.

[404] Online registration is possible in the case of a sole proprietorship. In accordance with the *Code of Commercial Partnerships and Companies*, since 2012, it has been possible to register a limited liability company online (in accordance with the so-called S24 procedure). In 2015, the option for registering general partnerships and limited partnerships online was introduced (using agreement templates provided by the Ministry of Justice). Applications for online registration are processed within one day. The moment of entering the data into the IT system is deemed to be the time of concluding the partnership agreement. To set up a company online, a qualified electronic signature or a signature confirmed with an e-PUAP trusted profile is required.

821. There are no sufficiently reliable data to estimate the illicit proceeds that can be laundered with certainty. However, using the estimates presented in chapter 5.2 on the potential illicit proceeds, which were calculated at the level of approx. 3.34% GDP, the threat of money laundering in this area should be assessed as very high.

822. Pursuant to data from the 2022 statistical yearbook of Statistics Poland, the number of crimes ascertained by the Police and prosecutor's office in completed preparatory proceedings in 2021 amounted to 829.102 and was by 7.0% higher compared to 2020, provided that more than a half i.e. approx. 50.5% was related to offences against property (i.e. set out in Articles 278-295 of the Penal Code), in particular fraud (i.e. referred to in Articles 286 and 287 of the Penal Code), which accounted for approx. 41.1% of this type of offences (approx. 20.7% of total crimes)[405] The number of offences against property increased compared to 2020 by approx. 12.9%, including the number of crimes – by approx. 29.1%. The share of crimes laid down in the *Act on counteracting drug addiction* amounted to approx. 7.5% (their number was by approx. 4.4% higher than in 2020).

823. According to information provided by the Central Investigation Bureau of the Police, in 2022 there were 181 crime groups eliminated in total, including 161 Polish and 20 international (in 2021 – 177 groups, including 163 Polish and 14 international, while in 2020 – 175 groups, including 150 Polish, 24 international and 1 Russian-speaking).[406] In this period, 2,292 suspects faced 2,316 charges with regard to Articles 258(1) and (2) of the Penal Code, i.e. participation in the organised crime group (i.e. by approx. 4.3% more suspects faced charges compared to 2021 and by approx. 24.8% more than in 2020), including:

- 2,042 members of the Polish groups (in 2021 – 1,986, in 2020 – 1,565),
- 249 members of the international groups (in 2021 – 199, in 2020 – 262),
- 1 member of a foreigners group (in 2021 – 2, in 2020 – 0),
- no member of the Russian-speaking groups (in 2021 – 11, in 2020 – 9).[407]

824. In 2021, 202 suspects faced 206 charges under Article 258(3) of the Penal Code (i.e. leading the group or association aimed at committing crimes). Thus, the increase in the number of suspects by approx. 6.9% was recorded compared to 2021 data and by more than 30.1% compared to 2020 data. This information referred to:

- 191 leaders of the Polish groups (in 2021 – 176, in 2020 – 138),
- 25 international leaders of the crime groups (w 2021 – 26, in 2020 – 27),

[405] Statistical Yearbook of the Republic of Poland 2022, Statistics Poland, Warsaw 2022, pp. 148-150, at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/

[406] Report on the activities of the Central Investigation Bureau of the Police for 2022 (statistical approach), p. 2; Report on the activities of the Central Investigation Bureau of the Police for 2021 (statistical approach), p. 2, Report on the activities of the Central Investigation Bureau of the Police for 2020 (statistical approach), p. 2, at: https://cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

[407] Report on the activities of the Central Investigation Bureau of the Police for 2022 (statistical approach), p. 4; Report on the activities of the Central Investigation Bureau of the Police for 2021 (statistical approach), p. 4, Report on the activities of the Central Investigation Bureau of the Police for 2020 (statistical approach), p. 4, at: https://cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

In addition, in 2020 1 Russian-speaking leader of the crime group faced charges under Article 258(3) of the Penal Code.

825. According to the Central Investigation Bureau of the Police data, the number of suspects charged with money laundering has also increased. In 2022, 1,042 charges were brought against 755 persons, which constitutes a decrease by approx. 4.9% compared to 2021 and the increase by approx. 19.5% compared to 2020.[408] This information demonstrates that the threat stemming from offences committed by crime groups does not decrease.

826. According to information provided by the National Prosecutor's Office, the greatest number of proceedings initiated in 2021 concerned computer fraud (i.e. offences under Article 287 of the Penal Code) – 21,581, followed by:

- offences under the *Act on counteracting drug addiction* – 21,314,
- burglary (i.e. offences under Article 279 of the Penal Code) – 20,924,
- fraud (i.e. offences under Article 286 of the Penal Code) – 20,038,
- theft (i.e. offences under Article 278 of the Penal Code) – 18,293,
- falsifying documents (i.e. offences under Article 270 of the Penal Code) – 17,096,
- destroying or damaging someone's property (i.e. offences under Article 288 of the Penal Code) – 16,411,
- appropriation (i.e. offences under Article 284 of the Penal Code) – 13,443,
- fraudulent use of someone's identity document (i.e. offences under Article 275 of the Penal Code) – 8,691,
- tax offences –5,849,

and many other.

827. Also in 2022, vast majority of the aforementioned categories was listed among 12 types of offences with the highest number of the initiated proceedings, i.e. fraud (i.e. offences under Article 286 of the Penal Code) – 96,170, theft (i.e. offences under Article 278 of the Penal Code) – 68,966, offences under the *Act on counteracting drug addiction* – 37,916, destroying or damaging someone's property (i.e. offences under Article 288 of the Penal Code) – 30,788, burglary (i.e. offences under Article 279 of the Penal Code) – 30,327, computer crimes (i.e. offences under Article 287 of the Penal Code) – 25,018, appropriation (i.e. offences under Article 284 of the Penal Code) – 19,148, falsifying documents (i.e. offences under Article 270 of the Penal Code) – 14,420, fraudulent use of someone's identity document (i.e. offences under Article 275 of the Penal Code) – 7,881 and tax offences – 3,742.[409]

---

[408] Report on the activities of the Central Investigation Bureau of the Police for 2022 (statistical approach), p. 4, Report on the activities of the Central Investigation Bureau of the Police for 2021 (statistical approach), p. 5, Report on the activities of the Central Investigation Bureau of the Police for 2020 (statistical approach), p. 4, at: https://cbsp.policja.pl/cbs/do-pobrania/raporty-z-dzialalnosci/9890,Raporty-z-dzialalnosci.html.

[409] It should be noted that the number of initiated proceedings in 2022 is nearly 5 times higher compared to the number of initiated proceedings in 2021 in the cases referring to the offences under Article 286 of the Penal Code and that the number of initiated proceedings in 2022is nearly 2 times higher compared to the number of initiated proceedings in 2021 in the cases referring to the offences under the *Act on counteracting drug addiction*, provided

828. A slightly different ordering of offences results from the analysis of the National Prosecutor's Office data with a view to the highest number of cases ended with an indictment or a motion for conviction in 2021 and in 2021, however the same categories of crimes continue to repeat i.e. the offences under the *Act on counteracting drug addiction* and under the *Fiscal Penal Code*, offences under Articles 224, 270, 275, 278, 284 and 286 of the Penal Code, as well as offences under Article 288 of the Penal Code.

Table 33. 10 types of offences with the highest number of cases ended with an indictment or a motion for conviction in 2021

Legal qualification	Number of cases ended with an indictment and a motion for conviction	Number of the indicted (persons with an indictment and a motion for conviction)
Act on counteracting drug addiction	13,431	30,193
Article 278 of the Penal Code	7,950	32,363
Article 270 of the Penal Code	7,762	11,386
Article 279 of the Penal Code	5,832	11,761
Article 288 of the Penal Code	5,169	11,268
Article 286 of the Penal Code	5,035	27,665
Article 284 of the Penal Code	3,778	6,039
Article 275 of the Penal Code	2,934	3,195
Penal Fiscal Code	2,915	4,984
Article 224 of the Penal Code	2,908	3,036

Table 34. 10 types of offences with the highest number of cases ended with an indictment or a motion for conviction in 2022

Legal qualification	Number of cases ended with an indictment and a motion for conviction	Number of the indicted (persons with an indictment and a motion for conviction)
Article 278 of the Penal Code	28,676	37,722
Act on counteracting drug addiction	20,328	28,962
Article 286 of the Penal Code	16,047	25,525

that in 2022 the number of cases ended with an indictment or a motion for conviction in the cases referring to the offences under Article 296 of the Penal Code was more than three higher and the number of cases ended with an indictment or a motion for conviction in the cases referring to the offences under the *Act on counteracting drug addiction* was more than 1.5 times higher.
Also the 4 times higher number of investigations initiated in 2022 compared to the number of investigations initiated in 2021 in the cases referring to the offences under Article 278 of the Penal Code as well as more than 2 times higher number investigations initiated in 2022 compared to the number of investigations initiated in 2021 in the cases referring to the offences under Article 288 of the Penal Code should be noted, provided that in 2022 the number of cases ended with an indictment or a motion for conviction in the cases referring to the offences under Article 278 of the Penal Code was more than 3.6 times higher and the number of cases ended with an indictment or a motion for conviction in the cases referring to the offences under Article 288 of the Penal code was nearly 1.8 times higher.

Article 288 of the Penal Code	9,241	11,617
Article 279 of the Penal Code	7,488	11,523
Article 270 of the Penal Code	5,192	7,568
Article 284 of the Penal Code	4,794	6,024
Article 275 of the Penal Code	2,524	3,171
Article 224 of the Penal Code	2,219	1,914
Penal Fiscal Code	1,909	4,904

829. Data of the National Prosecutor's Office on the amount of property seizures in 2021 indicate the following types of crime with the highest actual value of property seizures in total[410]: tax offences (i.e. offences laid down in the *Fiscal Penal Code*)[411], participation in the organised crime group (i.e. offences under Article 258 of the Penal Code), fraud (i.e. offence under Article 286 of the Penal Code), attestation of an untruth (i.e. offence under Article 271 of the Penal Code)[412], abuse of trust (i.e. offence under Article 296 of the Penal Code)[413], offences under the *Act on counteracting drug addiction*, credit/financial offence (i.e. offences under Article 297 of the Penal Code)[414], preventing or reduction of satisfaction of the creditors' claims (i.e. offences under Article 300 of the Penal Code), using the document attesting untruth (i.e. offences under Article 273 of the Penal Code) and appropriations (i.e. offences under Article 284 of the Penal Code).

830. In 2022, the highest actual value of the property seizures in total was recorded for the following types of offences[415]: tax offences (i.e. crimes laid down in the *Fiscal Penal Code*), participation in the organised crime group (i.e. offences under 258 of the Penal Code), fraud (i.e. offence under Article 286 of the Penal Code), credit/financial fraud (i.e. offences under Article 297 of the Penal Code**), passive corruption (Article 228 of the Penal Code),** offences under the *Act on counteracting drug addiction*, abuse of trust (i.e. offence under Article 296 of the Penal Code), **abuse of functions (Article 231 of the Penal Code)**, **intellectual forgery of invoices (Article 271a of the Penal Code),** attestation of an untruth (i.e. offence under Article 271 of the Penal Code).

[410] Without referring to the securities on property directly linked with money laundering (Article 299 of the Penal Code) and Article 294 of the Penal Code, which refers to committing various offences (i.e. under Article 278(1), (2), (5), Article 278a(1), Article 284(1) or (2), Article 285(1), Article 286(1) or (2), Article 287(1), Article 288(1) or (3), Article 290(1) or in Article 291(1) of the Penal Code) in relation to high-value property or property of particular importance to culture.

[411] It needs to be noted that according to data of the National Prosecutor's Office on the money laundering investigations initiated in 2019-2020, the most frequently identified offences – as the predicate offences – were those against tax obligations (approx. 34.7% in 2019 and approx. 32.0% in 2020).

[412] Offence under Article 271 of the Penal Code may be linked with fraud/extortion indicated by the GIFI, which refer to various types of fraud and extortion, including these committed with the use of documents attesting untruth.

[413] Offence under Article 296 of the Penal Code may be linked with the general category of fraud/extortion indicated by the GIFI as well as the acts to the detriment of a business entity.

[414] Offence under Article 297 of the Penal Code may be linked with the general category of fraud/extortion indicated by the GIFI.

[415] Without referring to the securities on property directly linked with money laundering (Article 299 of the Penal Code) and Article 294 of the Penal Code, which refers to committing various crimes (i.e. under Article 278(1), (2), (5), Article 278a(1), Article 284(1) or (2), Article 285(1), Article 286(1) or (2), Article 287(1), Article 288(1) or (3), Article 290(1) or in Article 291(1) of the Penal Code) in relation to high-value property or property of particular importance to culture

Table 35. Types of offences with the highest total amounts of property seizures according to data of the National Prosecutor's Office for 2021-2022 (in PLN)

2021		2022	
Legal qualification	**actual value of property seizures in total**	**Legal qualification**	**actual value of property seizures in total**
Penal Fiscal Code	1,691,231,999.97	*Penal Fiscal Code*	764,764,281.28
Article 258 of the Penal Code	394,580,260.79	Article 258 of the Penal Code	572,763,199.52
Article 286 of the Penal Code	371,739,395.72	Article 286 of the Penal Code	509,506,425.28
Article 271 of the Penal Code	200,338,922.12	Article 297 of the Penal Code	179,367,126.85
Article 296 of the Penal Code	160,723,108.11	Article 228 of the Penal Code	176,821,650.60
Act on counteracting drug addiction	121,004,437.87	*Act on counteracting drug addiction*	121,599,296.54
Article 297 of the Penal Code	106,298,109.18	Article 296 of the Penal Code	93,123,232.66
Article 300 of the Penal Code	66,330,291.92	Article 231 of the Penal Code	77,931,116.42
Article 273 of the Penal Code	59,693,338.75	Article 271a of the Penal Code	73,402,930.07
Article 284 of the Penal Code	54,834,450.05	Article 271 of the Penal Code	66,688,233.84

831. Also the data of the National Prosecutor's Office on the amount of property seizures for the previous period - 2019-2020 – demonstrate that the 11 types of crimes with the highest actual value of property seizures in total[416] include the offences under Articles 258, 271, 284, 286, 296 and 297 of the Penal Code, as well as the tax offences and offences under the *Act on counteracting drug addiction*.

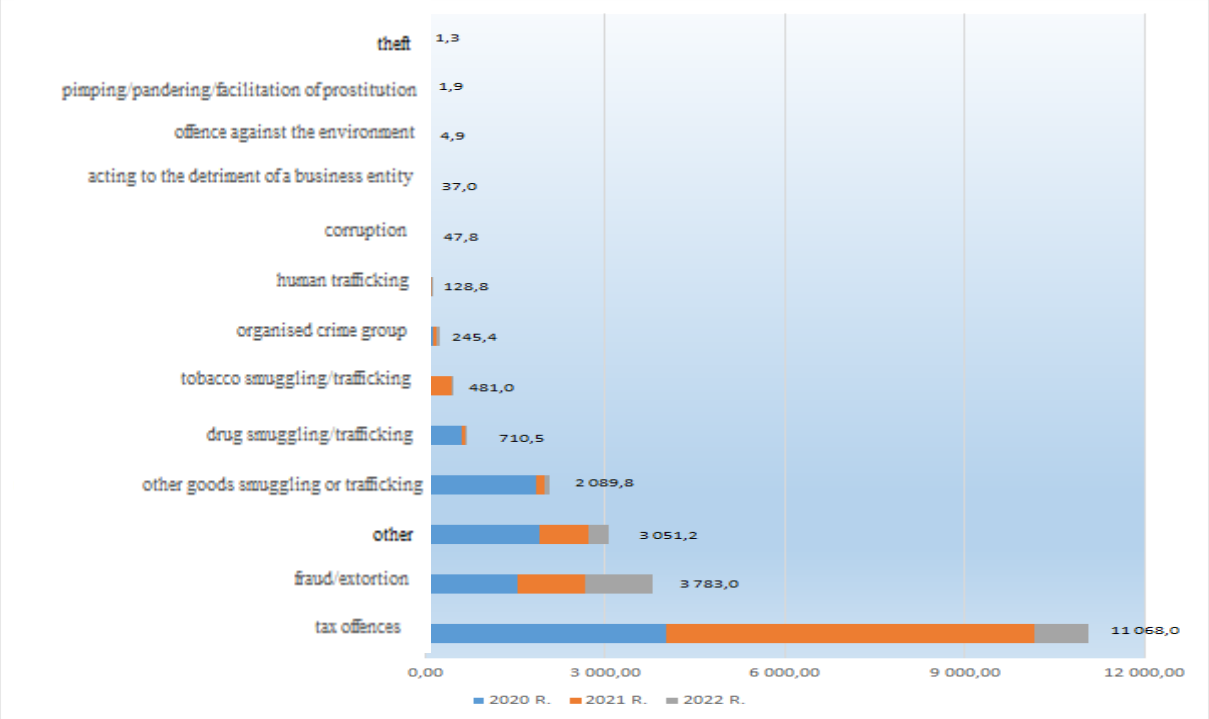
832. In general – based on National Prosecutor's Office data on the number of initiated cases, the number of cases ended with an indictment and the number of the indicted as well as the property seizures – it is possible to distinguish 4 types of crimes which are listed among the crimes with the highest actual values in all the a/m categories i.e. (ordered by the actual value of property seizures in total): tax offences, fraud (i.e. offence under Article 286 of the Penal Code), offences under *Act on counteracting drug addiction* and appropriations (i.e. offences under Article 284 of the Penal Code)[417]. In addition, the group of offences of the highest level of threat should include also the participation in the organised crime group (type of crimes ranked 2nd with a view to actual value of property seizures in total), among others due to the fact that crime groups are involved in a wide range of offences, including of economic nature.

833. These conclusions in the scope of 4 of 5 offences referred to above are confirmed by information of the Ministry of Justice for 2021-2022. According to the Ministry's data concerning the penal proceedings pertaining to the predicate offences for offences under Articles 165a and 299 of the Penal Code in the regional and district courts for 2021-2022, the most frequently identified crimes are the tax offences (approx. 14.0% of proceedings initiated in 2021 and approx. 9.7% of proceedings initiated in 2022), fraud (i.e. offences under Article

[416] Without consideration to the securities on property referring to Articles 299 and 294 of the Penal Code.
[417] The actual value of securities on property in 2022 for the offences under Article 284 of the Penal Code amounted to PLN 41,987,411.44 (being ranked at the 11th place in terms of value).

286 of the Penal Code – approx. 9.6% of proceedings initiated in 2021 and approx. 11.9% of proceedings initiated in 2022), participation in the organised crime group (i.e. offences under Article 258 of the Penal Code – approx. 7.6% of proceedings initiated in 2021 and approx.10.0% of proceedings initiated in 2022), attestation of an untruth (i.e. offences under Article 271 of the Penal Code – approx. 6.6% of proceedings initiated in 2021 and approx. 4.6% of proceedings initiated in 2022)[418], offences under the *Act on counteracting drug addiction* (approx. 3.0% of proceedings initiated in 2021 and approx. 2.1% of proceedings initiated in 2022).

Chart 35. Total value of suspicious transactions indicated in the GIFI notifications to the public prosecutors' offices by the types of the potential predicate offences in 2020-2022 (in PLN million)[419]



[418] The offence under Article 271 of the Penal Code may be linked with fraud/extortion indicated by the GIFI, which refer to various types of fraud and extortion, including these committed with the use of documents attesting untruth.

[419] According to information as of 13.03.2023, without references to the notifications, for which no potential predicate offence was identified.

834. According to the GIFI information for 2020-2022 concerning the potential predicate offences, to which the (main) notifications submitted by the authority to the public prosecutor's offices with regard to the suspected money laundering referred, the highest values of suspicious transactions were related to tax offences (including VAT fraud) and various types of fraud and extortion, followed by (excluding the cumulative group of the other crimes) – other goods smuggling or trafficking, drug trafficking, tobacco smuggling/trafficking[420], participation in the organised crime group and human trafficking.[421]

835. These conclusions are also supported by information on the potential predicate offences related to blockades of accounts and suspensions of transactions initiated by the GIFI. According to the graph below, the highest amounts of the total values of assets collected on the blocked accounts and the total values of suspended transactions may be linked to such types of predicate offences as: tax offences (including VAT fraud), various types of fraud/extortion, followed by (excluding the cumulative group of the other crimes) –corruption, acting to the detriment of a business entity, participation in the organised crime group, as well as other goods smuggling/trafficking and drug trafficking as well as human trafficking.[422]

Chart 36. Total value of assets on the blocked accounts and the values of suspended transactions by the types of offences for 2020-2022 (in PLN million)[423]

[420]Tobacco smuggling/illegal trading (as well as partially other goods smuggling/illegal trading) is linked with the breach of the *Penal Fiscal Code*, i.e. can be also linked with tax offences.

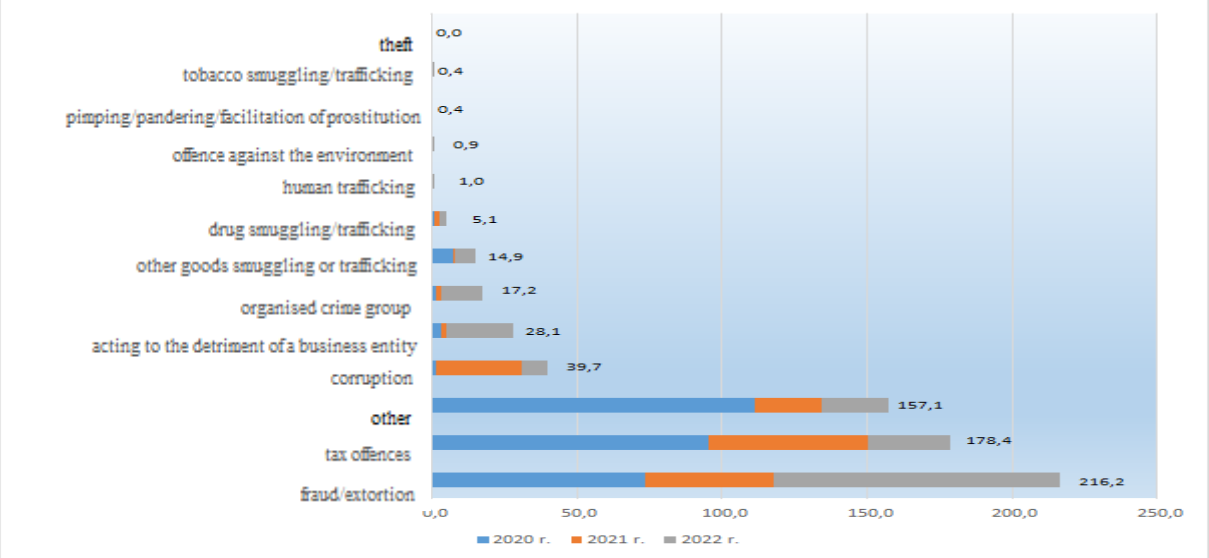
[421] The number of main notifications submitted by the GIFI in 2020-2022 indicates that in most cases they referred to fraud and extortion (approx. 45.0% of all main notifications), tax offences (approx. 32.1% of all main notifications), other goods smuggling/illegal trading (approx. 3.1% of all main notifications), participation in the organised crime group (approx. 2.9% of all main notifications) and drug trafficking/trading (approx. 1.2% of all main notifications), human trafficking (approx. 0.8% of all main notifications), as well as corruption and acts to the detriment of a business entity (approx. 0.7% of all main notifications).

It should be additionally noted that the share of main notifications on money laundering from the potential fraud/extortion in the general number of these notifications in a given year continues to grow (from approx. 38.8% in 2019 to more than a half of all main notifications in 2022), with simultaneous decrease of main notifications on money laundering from the potential tax offences (from approx. 43.1% in 2019 to slightly above ¼ of all main notifications in 2022).

At the same time, a certain increase in the number of main notifications related to such potential predicate offences as participation in the organised crime group (approx. 5.8% of all main notifications in this year) and human trafficking (approx. 2.5% of all notifications in this year) was recorded compared to data from the previous years.

[422] Tobacco smuggling/trading and human trafficking were linked to blockades of accounts and suspensions of transactions in 2020-2022 of the total value corresponding to approx. PLN 0.4 million and approx. PLN 1.0 million respectively.

[423] According to information to information as of 13.03.2023, without references to blockades of accounts and suspensions of transactions, for which no information on the potential predicate offence was assigned.



836. It should be also noted that in the event of request for information sent by the GIFI abroad to the foreign partners – although a large part of them referred to the cases with no indications as to the potential predicate offence for money laundering (approx. 38.8% for requests in 2021 and approx. 40.3% for requests in 2022) – it can be stated that in context of the remaining cases, to which the requests referred, the most frequently indicated potential predicate offences included fraud/extortion (approx. 32.8% of all requests in 2021 and approx. 35.5% of all requests in 2022)[424] and tax offences (approx. 13.0% for all requests in 2021 and approx. 9.8% of all requests in 2022). In addition – apart from the aforementioned categories of offences – the 5 most frequently identified predicate offences for money laundering included:

- in 2021: drug trafficking (approx. 4.3% of all requests), corruption (approx. 4.1% of all requests), participation in an organised crime group (approx. 1.4% of all requests),
- in 2022: participation in an organised crime group (approx. 4.0% of all requests), human trafficking (approx. 1.8% of all requests), other goods smuggling or trafficking (approx. 1.8% of all requests).

837. With regard to the requests for information received by the GIFI from the foreign partners, they also most frequently refer to the following predicate offences for money laundering:

- in 2021: fraud (approx. 50.7% of all requests), tax offences (approx. 7.7% of all requests), illegal traffic in narcotic drugs and psychotropic substances (approx. 4.0% of all requests), corruption (approx. 2.6% of all requests), human trafficking (approx. 1.4% of all requests,
- in 2022: fraud (approx. 43.6% of all requests), tax offences (approx. 11.3% of all requests), embezzlement (approx. 4.5% of all requests), trafficking in narcotic drugs and

[424] Including investment fraud, fraud related to extortion of access data to the financial products, including so called *Business Email Compromise*.
It should be noted that even if 2018 – according to the 2019 National Risk Assessment – the share of the GIFI requests for information to the foreign FIUs associated with the cases related to the potential laundering of the proceeds of crime applied only to approx. 13.5% of all requests.

psychotropic substances (approx. 3.3% of all requests), corruption (approx. 1.3% of all requests)[425].

838. As demonstrated by the data contained in this document, the threat of crime continues to be significant, in particular with regard to tax offences, various types of fraud/extortion, including these related to attestation of an untruth or financial fraud, participation in the organised crime groups, offences under the *Act on counteracting drug addiction*. One should also mention the significance of threat of corruption. According to the Central Anti-Corruption Bureau data, the material gains and the value of property seizures revealed by the service during its operations in 2019-2021 had the value of hundred thousands of Polish zlotys, while the losses in the property of the State Treasury revealed during the operational – intelligence proceedings – in billions of Polish zlotys[426].

839. For the above-mentioned reasons, the threat of predicate offences for money laundering – similarly as in the 2019 National Risk Assessment – should be assessed at the level between medium and high.

840. In its report on the supranational assessment of the risk of money laundering and terrorist financing of 27 October 2022, the European Commission determined no general level of threat of money laundering for the EU.[427] Instead, it identified 43 products and services in 8 areas, which are potentially vulnerable to the risk of money laundering and terrorism financing and determined the levels of threat and vulnerability for them (separately for money laundering and terrorism financing). The assessments for certain products and services were subject to a certain adjustment compared to 2019 (e.g. for "crypto-assets" previously identified as "virtual currencies and other virtual assets" or "*on-line* gambling").[428] On the basis of assessment of the described products/services it can be assumed that the risk of money laundering in the EU is at the high level.[429]

841. Among the entities[430] present in the GIFI notifications to the public prosecutor's office submitted in 2020-2022 with regard to the suspected money laundering and for which the country of citizenship/registration was identified, the vast majority were the Polish entities

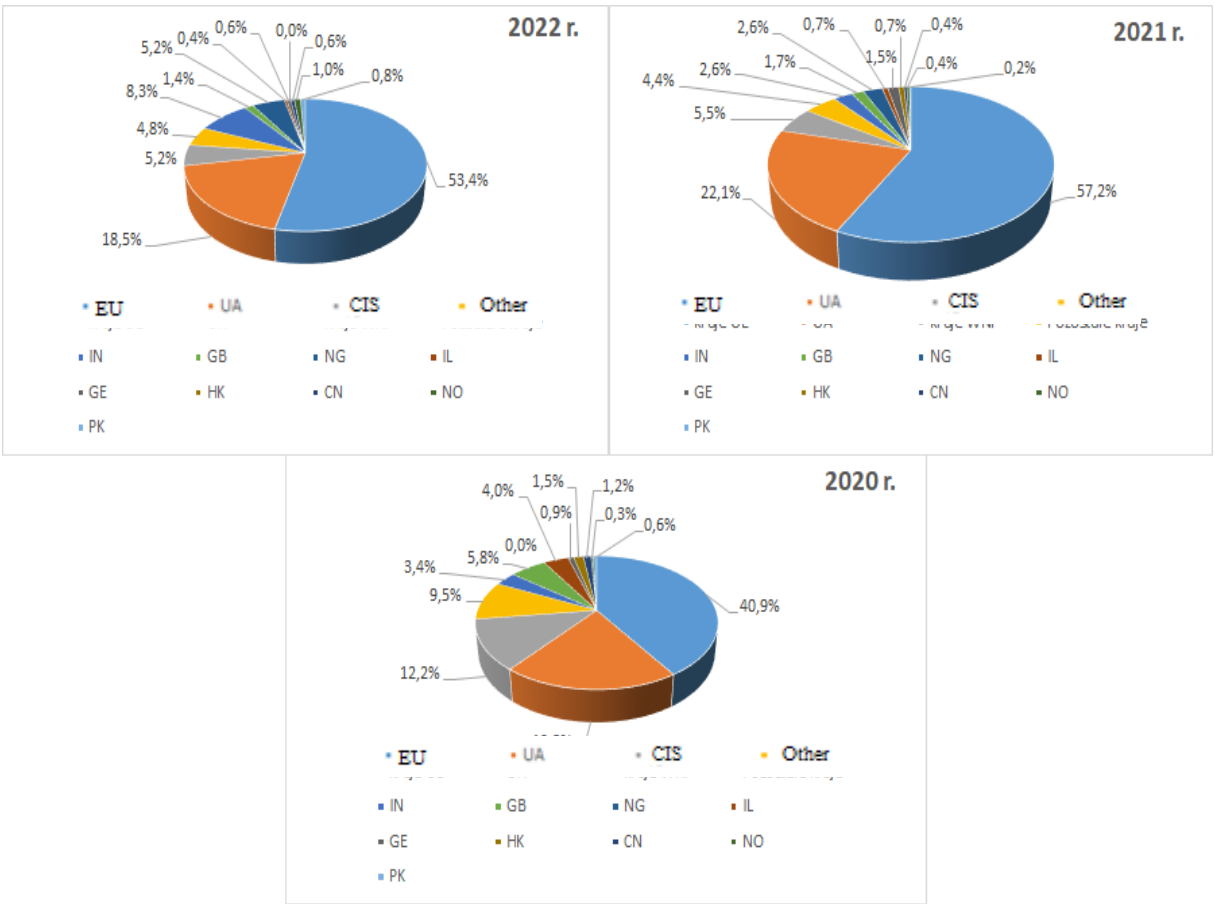
[425] In 2022, a certain group was also formed by the requests for information on avoiding the financial/economic sanctions (approx. 1.5% of all requests).
[426] Vide data in sub-chapter 5.1.4, as well as: Information on the operational results of the Central Anti-Corruption Bureau in 2021, p. 10 (at: https://www.cba.gov.pl/pl/o-nas/informacja-o-wynikach).
[427] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 27.10.2022, at: https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en.
[428] Commission staff working document accompanying the document report from the commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 27.10.2022, at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0344.
[429] In contrary to the previous one, the European Commission presented in the supranational assessment of the risk of money laundering and terrorist financing of 2022 not only the levels of threat and vulnerability of money laundering and threats and vulnerabilities of terrorism financing for each product/service, but also estimated the risk of money laundering and terrorism financing for each of them. Based on the latter, the average level of risk of money laundering would amount to approx. 3.0 (in the four scale rating), while the average level of risk of terrorism financing – to approx. 2.2.
[430] I.e. natural persons and business entities.

(approx. 54.3%). In the remaining cases, the entities from the following countries were identified:

- other EU countries (approx. 22.4%),
- Ukraine (approx. 8.7%),
- CIS (approx. 3.0%),
- Vietnam (approx. 2.5%),
- India (approx. 2.2%),
- Nigeria (approx. 1.3%),
- the United Kingdom (approx. 1.1%).

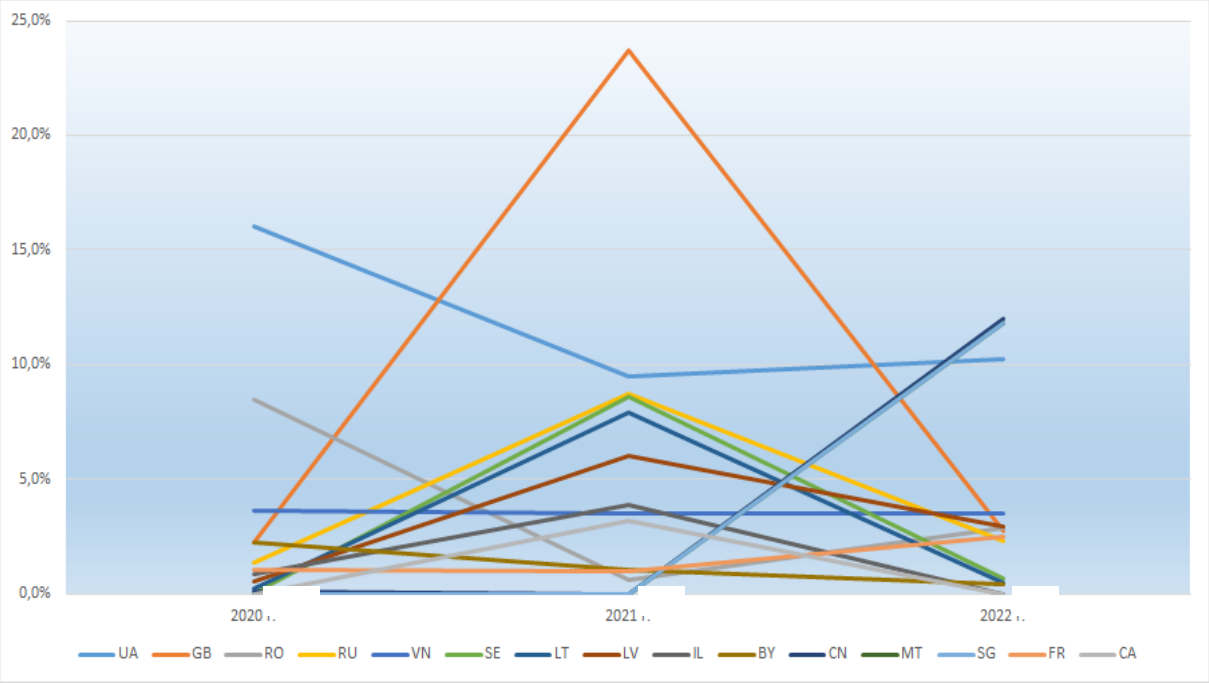
842. With regard to the EU countries, the most frequently identified entities originated from Italy (approx. 3.4%), Hungary (approx. 3.0%), Latvia (approx. 2.8%), France (approx. 2.0%), Germany (approx. 1.6%), Romania (approx. 1.5%) and the Kingdom of Netherland (approx. 1.1%), while with regard to the CIS countries, these were mostly the entities from Russia (approx. 1.2%) and Belarus (approx. 1.1%).

Chart 37. Percentage of the foreign entities from particular countries/groups of countries in the total number of foreign entities, activity of which was described in the GIFI notifications submitted to the public prosecutor's offices in 2020-2022



843. If we consider the amounts of suspicious transactions described in the GIFI notifications to the public prosecutor's office, the ranking of countries from which the entities indicated in these notifications originate, will change significantly. The countries with the highest percentage in the total number of suspicious transactions indicated in the GIFI notifications to the public prosecutor's office in 2020-2022 include Ukraine (approx. 13.2%), the United Kingdom (approx. 9.1%), Romania (approx. 5.3%), Russia (approx. 3.8%), Vietnam (approx. 3.6%), Sweden (approx. 2.9%), Lithuania (approx. 2.7%) and Latvia (approx. 2.6%), Italy (approx. 1.7%) and Belarus (approx. 1.6%).

Chart 38. Percentage of the amounts of suspicious transactions indicated in the GIFI notifications submitted to the public prosecutor's office in 2020-2022 by countries, from which the foreign entities listed in these notifications originate (15 countries with the highest percentage)



844. The scale of exchange of information with particular foreign partners of the GIFI in the area of individual analytical proceedings related to the suspected money laundering or terrorism financing forms a certain reflection of the threats stemming from cross-border financial flows.

The requests for information have been mostly sent to the financial intelligence units from the countries, in which the suspicious transactions were made or from which the entities or accounts otherwise linked with suspicious activity originated. The requests for information have been received primarily from the countries where suspicious transactions related to the funds originating from Poland or other links with the Polish entities or accounts were identified.

845. The countries with which the most intensive information exchange was carried out include the countries from which the entities indicated in the GIFI notifications to the public prosecutor's office have most frequently originated (i.e. Ukraine, Germany, Italy, France as well as Latvia, Hungary and the Kingdom of Netherlands). It needs to be noted that the GIFI has also conducted the dynamic information exchange with the United Kingdom – which was identified among the countries, from which the entities indicated in the GIFI notifications to the public prosecutor's office with the highest percentage in the total amount of suspicious transactions have most frequently originated.

846. With regard to the requests for information submitted to the GIFI, they were most frequently obtained from the EU Member States (more than 2/3 of all requests in 2020-2022), followed by Ukraine, CIS countries[431], the United Kingdom and the USA, provided that it needs to be noted that even if the percentage of requests from Ukraine has increased on a year by year basis, a drop was recorded for the CIS countries.

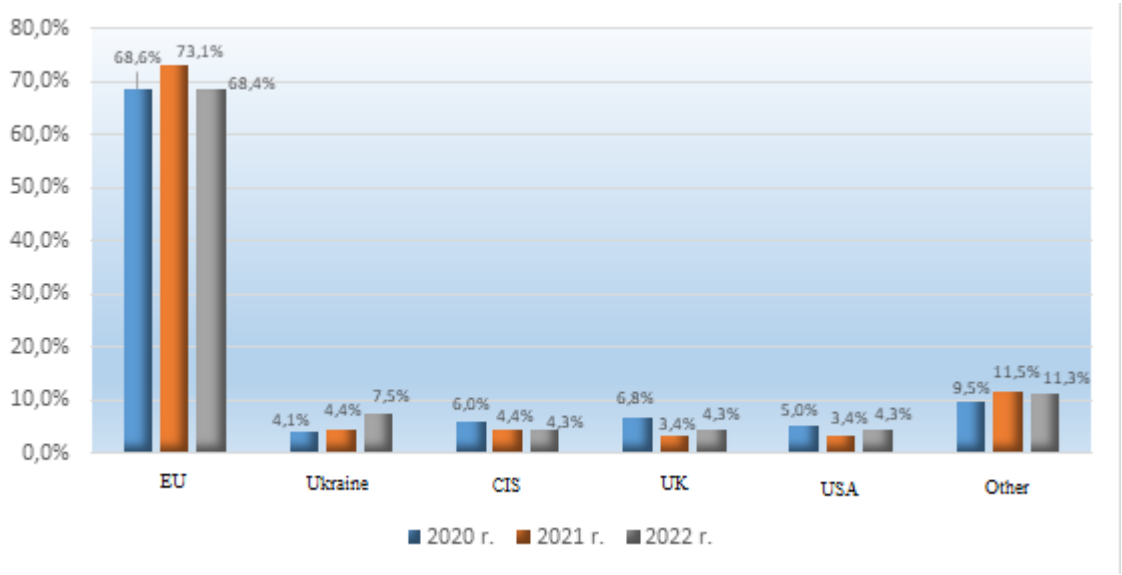
847. From among the EU countries, the highest number of requests for information was received from:

- Germany, France, Lithuania, Italy, Latvia, Luxembourg and Hungary – in 2020 (approx. 62.7% of requests from the EU),
- Germany, France, Lithuania, Italy, Malta, Luxembourg and the Kingdom of Netherlands – in 2021 (approx. 63.1% of requests from the EU),
- Germany, France, Latvia, Italy, Slovakia, Lithuania and the Kingdom of Netherlands – in 2022 (approx. 70.3% of requests from the EU).

848. As can be seen, in 2020-2022 the countries from which the highest number of requests for information was sent each year included Germany, France and Italy, i.e. three the most densely populated EU countries, as well as Lithuania.

Chart 39. Percentage of requests for information from particular countries/groups of countries in the total number of requests for information received by the GIFI in 2020-2022

[431]The list of CIS countries, from which the highest number of requests was obtained, has changed depending on the year – in 2020 it was Moldova and Russia with approx. 1.6% and approx. 1.4% of all requests respectively, which was repeated also in 2021 with approx. 2.6% and approx. 0.8% of all requests respectively, while in 2022 the highest number was recorded for Kazakhstan, Moldova and Uzbekistan with approx. 1.5%, approx. 1.0% and approx. 0.8% of all requests respectively.



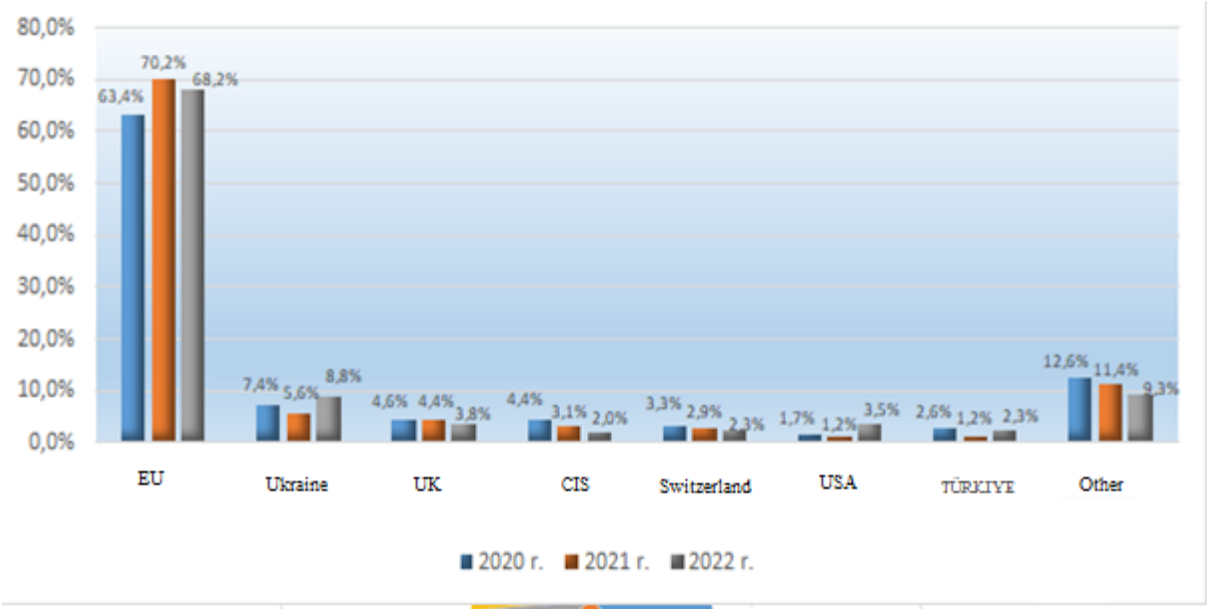
849. With regard to the requests for information submitted by the GIFI, they were most frequently sent to the EU countries, followed by Ukraine, the United Kingdom, CIS[432], Switzerland, USA and Türkiye. In the case of the EU countries, the highest number of requests was submitted to:

- Germany, Czech, Estonia, Lithuania, Latvia, the Kingdom of Netherlands, Hungary and Italy – in 2020 (approx. 55.6% of all requests to the EU),
- Germany, Lithuania, France, Spain, Czech, Latvia and Hungary – in 2021 (approx. 55.5% of all requests to the EU),
- Germany, Lithuania, Czech, Belgium, Spain and Hungary – in 2022 (approx. 54.0% of all requests to the EU).

850. As can be seen, in 2020-2022 the countries, to which the highest number of requests for information was sent each year, included Germany, Czech and Lithuania (i.e. the Poland's neighbours).

Chart 40. Percentage of requests for information to particular countries/groups of countries in the total number of requests for information submitted by the GIFI in 2020-2022

[432] The list of CIS countries, to which the highest number of requests was sent, has changed depending on the year – in 2020 it was Russia and Belarus with approx. 2.2% and approx. 1.2% of all requests respectively, which was repeated also in 2021 with approx. 1.9% and approx. 1.0% of all requests respectively, while in 2022 the highest number was recorded for Kirghizstan, Azerbaijan and Moldova with approx. 0.5% of all requests respectively



851. Annex No. 3 to this documents presents the analysis of the above-threshold transactions for 2020-2022, in context of their flow directions. It should be noted that a part of countries indicated both as these, from which the greatest amounts were transferred to Poland and these, to which the greatest amounts of funds were transferred, overlap with the jurisdictions describe above with regard to the exchange of information between the GIFI and its counterparts i.e.:

- the EU (including in particular Germany, France and the Kingdom of Netherlands), the United Kingdom, the USA, Switzerland, Ukraine (in the case of the inbound above-threshold transactions), with the exception of the EEA countries (Island and Norway) not listed among the countries, with which the GIFI has exchanged the greatest volume of information,
- the EU (including in particular Germany, France and the Kingdom of Netherlands), the United Kingdom, the USA, Switzerland, Ukraine (in the case of the outbound above-threshold transactions), with the exception of China and Russia not listed among the countries, with which the GIFI has exchanged the greatest volume of information.

852. According to the analysis of the above-threshold transactions, the value of above-threshold outbound transfers to the countries applying harmful tax competition has been increasing on a year by year basis, while the value of transactions grows by more or less the same value on a year by year basis. It is possible, that among these transfers there are many linked with hiding the illicit proceeds or with avoiding taxation.

853. The analysis of declarations of foreign currency from 2021-2022 (see Chapter 7.2.2), information of which are collected in the CIS, confirms the intensity of transfer of funds by the Ukrainian entities (the highest total value of cash imported to the EU was declared by the citizens of this state, and also the Ukrainians – next after the Polish citizens – have declared the highest total value of cash exported from the EU), which cannot be surprising, taking into account massive Ukrainian migration in Poland and relatively wide-scale economic relationships with Ukraine. A high number of declarations of foreign currency concerning the export of cash from the EU to Türkiye and Morocco may be surprising, provided that the citizens of this stage – following the Poles and Ukrainians – have declared the foreign currencies of the highest total value of cash exported from the EU.

854. According to information on the content of national assessments of the risk money laundering and financing of terrorism of the other countries, Poland was only occasionally indicated as one of the main countries of origin of the illicit assets or to which such assets are transferred. On the basis of verifications of the national assessments of the risk money laundering and financing of terrorism of the other countries published since 2019 (primarily the analyses of documents of the EU Member States and other neighbours of Poland) it was stated that at least one report on the national assessment of the risk money laundering and financing of terrorism of the other country of 2019 indicates that Poland generates a medium threat of money laundering for this country (i.e. at the level 3 in the five scale rating).[433] In addition, at least 2 countries indicated in their analyses the examples of money laundering cases, which referred among others to the Polish entities or accounts. In this context, the medium level of threat may be referred to.

855. Based on information referred to above, the level of threat of money laundering in Poland can be estimated, in particular with a view to the threat of predicate offences for money laundering, at least at a high level (i.e. at the level 3 in the four scale rating).

Level of vulnerability

856. The 2019 NRA indicated that there have been a few types of products and services in Poland that may directly facilitate making quick and anonymous transactions. At present, the situation is similar, however one should note the relatively quick development of the virtual assets market. The new virtual currencies as well as products and services based on such virtual currencies, a part of which demonstrates the features enhancing relatively effective hiding of personal data of the users, continue to appear. In addition, the opportunity to transfer virtual currency directly between the users, without the intermediation of the entities applying the KYC software, is also of importance.

857. It is also worth to note that although the virtual currency service providers are obliged to comply with the anti-money laundering and counter-terrorism financing provisions and are subject to relevant controls, the easiness of access to the portals offering the purchase or exchange of cryptocurrencies and related services registered outside the EU enhances the increase of the risk of use of virtual currencies for money laundering.

858. Although the observed development of non-cash transactions significantly limits the cash transaction market, cash still has a significant share in the aggregate money supply M1[434]. The continuous presence of cash in ordinary economic trading as a medium of exchange as well as a means of accumulating savings[435] is associated with the risk of its use for criminal purposes.

---

[433] Erste Nationale Risikoanalyse 2018/2019 - Anlage 4: Grenzüberschreitende Bedrohung, Federal Ministry of Finance, Berlin (Germany) October 2019, at: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.html.

[434] Despite the decreases in the previous years to the level of 19.7% in 2021, the share of cash in Poland within the aggregate money supply M1 was by approx. 6.1 percentage points higher compared to the European Union average (*Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2021 r.*, National Bank of Poland, December 2022, pp. 40-41, at: https://nbp.pl/system-platniczy/dane-i-analizy/analizy-i-opracowania/obrot-bezgotowkowy/).

[435] According to the analysis of the National Bank of Poland: "The phenomena caused by the COVID-19 pandemic have contributed to the increased cash demand, which in turn resulted in the intensified withdrawals of cash by the consumers, which was frequently accompanied by accumulating savings" (Raport o obrocie gotówkowym w

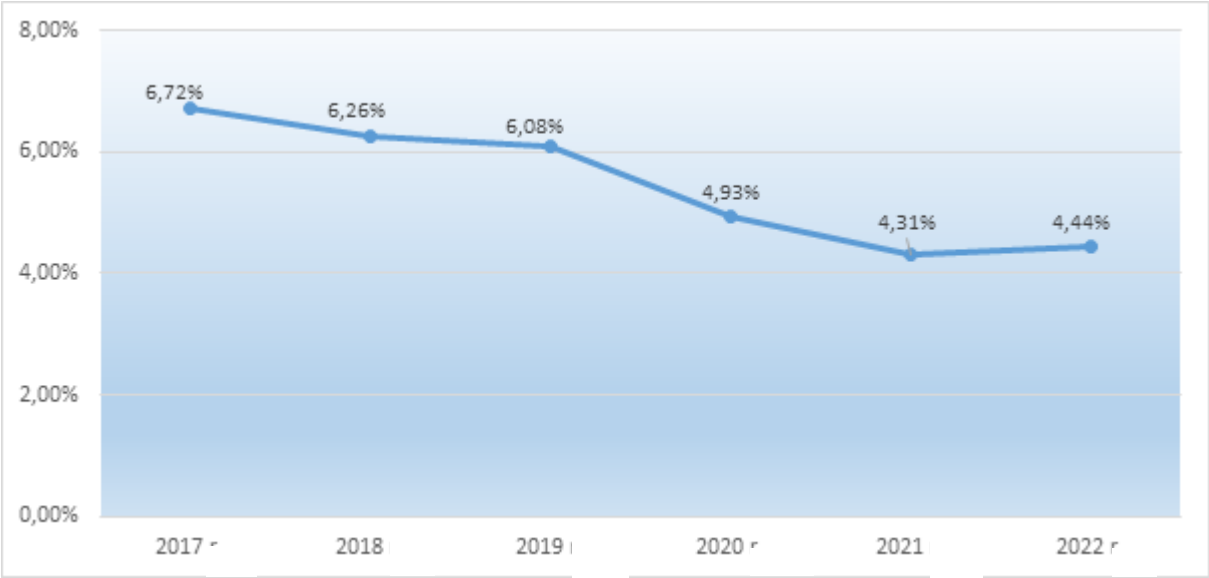
In context of products and anonymity enhancing services, one should also point out at the opportunities to make cash transactions by practically anonymous persons, when making so called occasional transactions below the threshold of EUR 15,000 (or EUR 10,000 in the case of obligated institutions referred to in Article 2(10(21-23) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*). Such transactions – in particular when combined with the other products and services (see for example information contained in chapter 5.1. in the sub-chapter "Illegal traffic in narcotic drugs and psychotropic substances") – create vulnerability to money laundering.

859. According to the analysis of information on the above-threshold transactions submitted by the obligated institutions to the GIFI, they include relatively few transactions classified by the obligated institutions as cash deposits or withdrawals. In addition, a downward trend is observed – between 2017 and 2022 this share decreased by 2.28 percentage point. This may result from several factors, in particular from:

- the existing and continuously appearing other – quicker and easy – transactions methods with the use of products and services provided by the banks and payment institutions,
- willingness to ensure security of storage and transfer of high-value funds,
- mandatory provisions of Article 19 of the *Act of 6 March 2018 – Economic Operators' Law,* specifying the threshold above which a transaction – in the case of making or accepting payments linked with the performed business activity between economic operators – has to be made only by means of a payment account of the operator,
- the provisions of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in the scope of implementation of customer due diligence by the obligated institutions and its potential impact – in the case of cash transactions made by the customer of an obligated institution – on the assessment of risk related to the business relationships or an occasional transaction.

Chart 41. Percentage of transactions classified by obligated institutions as cash deposits or withdrawals in the total number of the above-threshold transactions submitted by these institutions in 2017-2022

Polsce w 2020 r., National Bank of Poland, Warsaw 2021, p. 36, at: https://nbp.pl/publikacje/cykliczne-materialy-analityczne-nbp/raporty-o-obrocie-gotowkowym/).



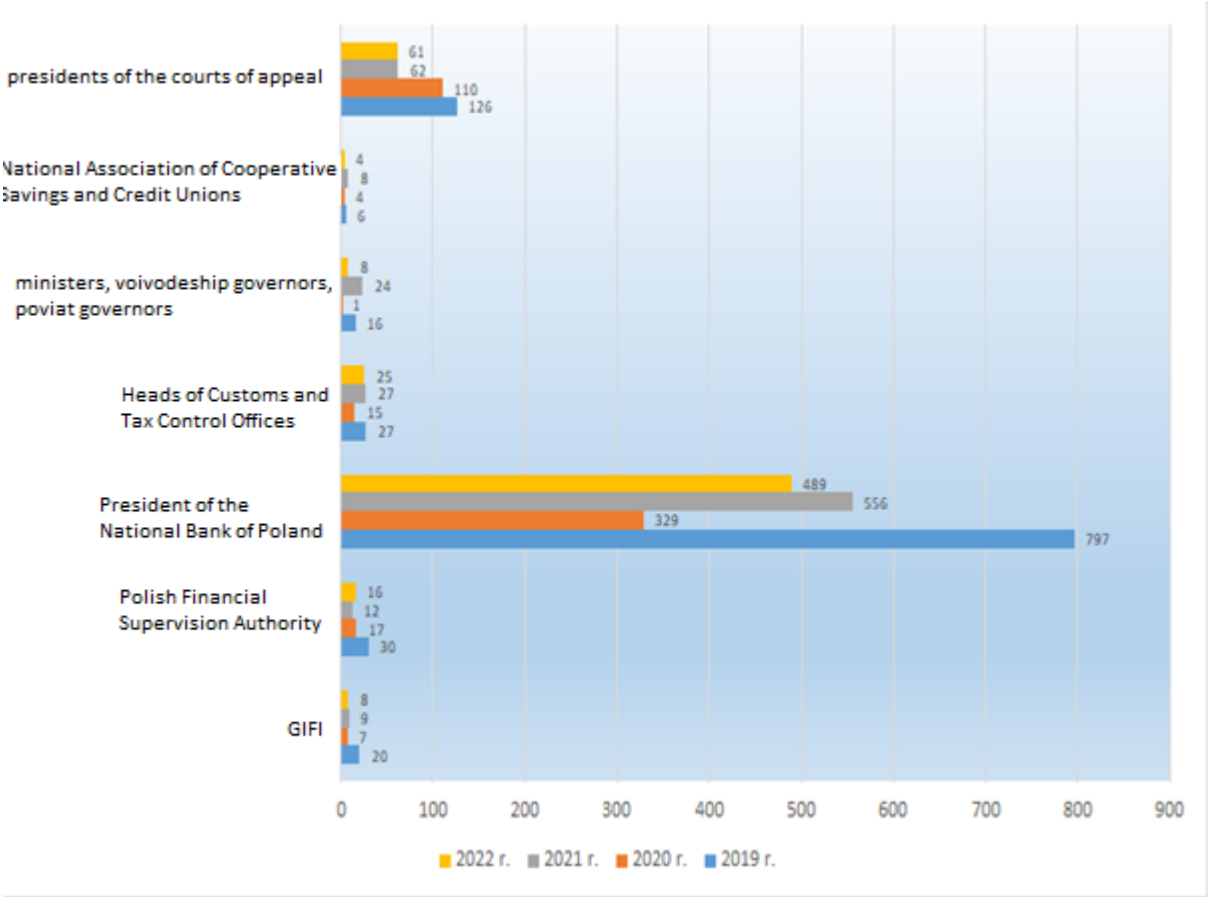
860. In context of products and services that may directly facilitate quick and anonymous transactions, one should also remember the vulnerability linked to the "collect" type services (see chapter 7.2.1. – "Vulnerability of the financial market" and the description in the "Banking" section). Their use impedes the analyses of suspicious financial flows and access to knowledge on the actual payer and recipient of the transfer

861. In the contemporary globalised world, transactions from Poland to another country and vice versa pose practically no difficulties. Therefore, their adequate verification as well as verification of the persons and entities making the transaction is of importance. The provisions implemented in 2018 and later amendments of the provisions on anti-money laundering and counter-terrorism financing have significantly contributed to the specification of the scope and rules of monitoring of the flow channels of money as well as of the other assets, in particular virtual currencies.

862. A vast majority of the categories of entities that should be the obligated institutions, are covered by the anti-money laundering and counter-terrorism financing provisions and supervision in this area. The obligated institutions are generally aware of their AML/CFT obligations (however their awareness may differ depending on the category of the institution and between particular entities), including in the scope of analysing the transactions and applying customer due diligence and reporting information on their suspicions to the GIFI. The supervisory authorities verify information on the potential non-compliance of the operation of these entities with the regulations.

863. On the basis of information referred to above, the level of vulnerability of the economy can be estimated as medium.

Chart 42. Number of controls of compliance with the anti-money laundering and counter-terrorism financing provisions by the obligated institutions in 2019-2022



864. According to information published in the GIFI report, the number of controls of compliance with the anti-money laundering and counter-terrorism financing provisions by the obligated institutions decreased in 2020 compared to the previous period. The main reason behind this was the restrictions related to the pandemic and adaptation of the supervisory authorities to operation in the new conditions. It should be noted that although the number of these controls has increased starting from 2021, it still fails to reach the 2019 level for a majority of the authorities. This results among others from a focus on identification of the obligated institutions for control purposes (based on the risk-based approach principle), operation of which may be the most exposed to the risk of money laundering or terrorism financing and on more thorough verification.[436, 437]

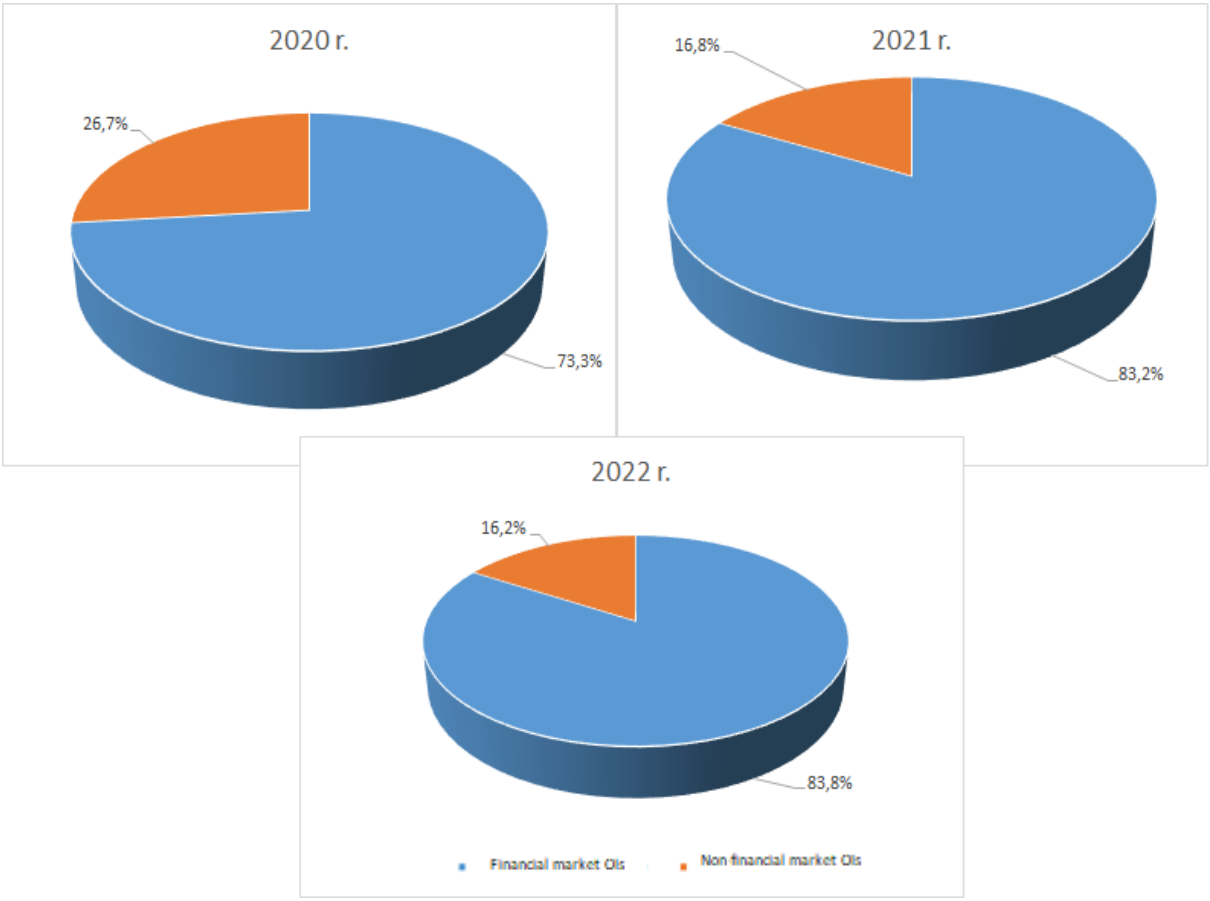
865. A vast majority of the obligated institutions controlled in 2020-2022 with a view to compliance with the anti-money laundering and counter-terrorism financing provisions are classified as the financial market institutions (from 73.3% in 2020 to 83.8% in 2022). This results among others from the scope of operation of the institutions with control powers. Three of them i.e. the Polish Financial Supervision Authority, National Bank of Poland and the National Association of Cooperative Savings and Credit Union, control only the obligated

[436] With regard to the GIFI, in 2020-2022 a positive assessment was provided only for 2 inspections in the post-inspection statements, in the remaining cases the following assessments were granted: positive with deficiencies (6), positive with irregularities (5), negative (11).

[437] It should be also noted that - with regard to the GIFI – in 2022 the organisational changes were introduced to decrease the workload of the control staff and eliminate the tasks not directly associated with the controls or cooperation with the other supervisory authorities as well as to increase the number of controllers. Within 5 months, up to March 2023, the number of employees of the Control Division of the Department of Financial Information of the Ministry of Finance was increased by approx. 22.2%.

institutions in the financial market, provided that the National Bank of Poland, controlling only the currency exchange office operators, performs the highest number of controls.

Chart 43. Breakdown of the obligated institutions controlled in 2020-2022 by the operation on the financial market or outside the financial market



866. During the controls performed by the GIFI as well as by the other authorities and entities listed in Article 130(2)(1) of the Act referred to above, the cases of irregularities in the area of fulfilment of the obligations provided for in the anti-money laundering and counter-terrorism financing provisions by the obligated institutions, although it needs to be remembered that their type and weight does not always require to initiate and administrative procedure with the aim to impose a penalty. In effect of the initiated administrative procedures, both the financial sector and non-financial sector institutions have received financial penalties[438]. According to the GIFI data, in 2021-2022 the penalties were most frequently imposed for breaches of the following provisions:

- Articles 7-8, Article 27(3), Article 33 with regard to Article 34(1)(1-4), Article 43, Article 46(2)(1), section 2(1) and (3), Article 50, Article 52, Article 53, Article 72, Article 74 and Article 76 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* (in 2022),

[438] Dedicated information is published on the official website of the Ministry of Finance in the GIFI tab (including information on the penalties imposed by the President of the National Bank of Poland) and on the KNF website.

- Article 8, Article 27 ust.3, Article 33 with regard to Article 34(1)(2), clause 4(a-b), Article 43, Article 46, Article 50, Article 52, Article 53, Article 72, Article 74 and Article 76 of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* (w 2021).

867. The public administration authorities involved in the national anti-money laundering system, in particular the supervisory authorities performing supervision over the particular categories of the institutions, the GIFI, as well as law enforcement agencies have relevant knowledge on the risk of money laundering and terrorism financing. This results among others from various statements, reports and information on the particular cases published by these authorities.

868. According to information, in vast majority of cases the authorities supervising the obligated institutions have adequate resources to control these entities. All supervisory authorities provide information on the performed controls to the GIFI, and the results of the performed control form the basis to impose the administrative sanctions and apply other supervisory instruments to the obligated institutions. Pursuant to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, the GIFI takes the actions to coordinate the control activities of the other supervisory authorities. Cooperation between the GIFI and the Office of the KNF and their foreign counterparts is at a high level.

869. Based on information referred to above on the operation of authorities supervising the obligated institutions, the assessed vulnerability is at the level between low and medium.

870. The GIFI is well aware of the risk of money laundering and terrorism financing. In addition, it is relatively well capable of collecting and analysing information on the suspicious activities and transactions i.e.:

- has direct or indirect access to most databases of the public administration authorities, necessary to analyse information on the suspicious activities and transactions,
- has powers to receive additional information on request from the obligated institutions and cooperating units,
- in recent times, the number of trainings/workshops dedicated to the employees in the area of the GIFI competences[439] has increased (including at the international level).

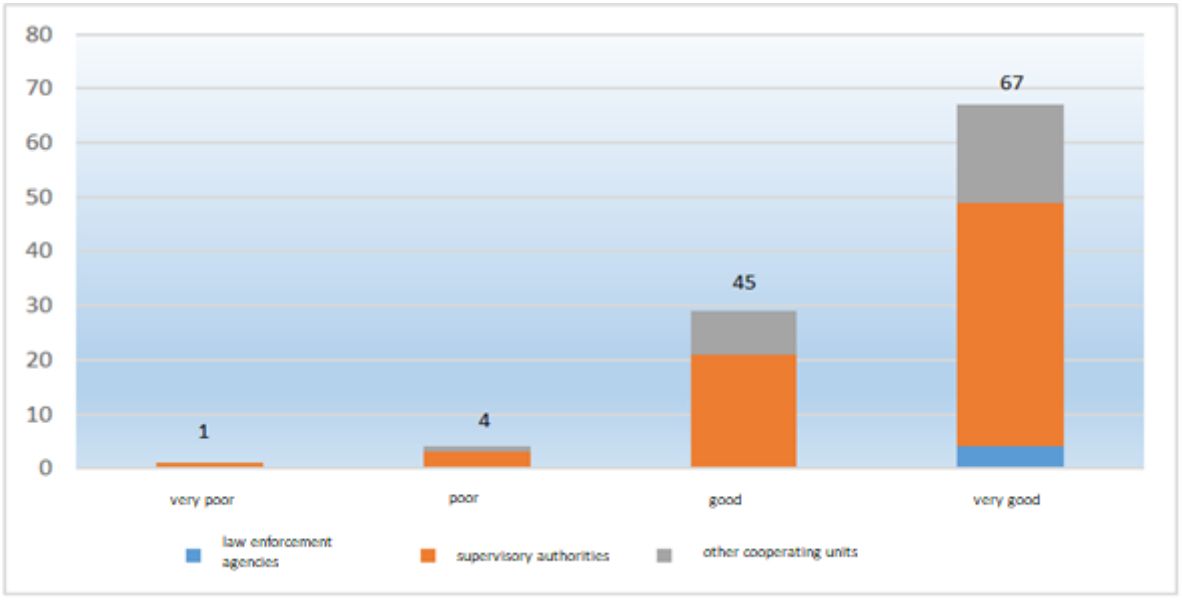
871. In addition, the employment in the Department of Financial Information of the Ministry of Finance has been increasing on a regular basis starting from 2017. Human resources allocated to the implementation of anti-money laundering and counter-terrorism financing tasks increased by approx. 49.2% (taking into account the number of jobs) between 2017 and 2022, According to the assessment of performance of tasks assigned to this unit, this percentage value should further grow. Further development of the IT system of the GIFI to increase its effectiveness is planned. The operation of the Department is financed from the Ministry of Finance budget to a sufficient extent.

872. Exchange of information between the GIFI and other cooperating units, in particular law enforcement agencies, is relatively efficient, primarily in terms of providing information by the GIFI on request (information is not limited in terms of scope and type of data and the

[439] In 2022, the employees of the Department of Financial Information of the Ministry of Finance participated, among others, in training on OSINT as well as blockchain technologies and cryptocurrencies.

type of law enforcement or justice authority). In 2022, the GIFI responses were provided within approx. 11 days in average [440] (although a half of responses was sent within 3 days from the registration of the case on the basis of the received request[441]). Despite a relatively short period of generating the response, development of the ICT system for information exchange (primarily with all law enforcement agencies) and preparation of the e-document templates to further speed up the transfer of requests and responses seem to be reasonable.

Chart 44. Assessment of cooperation with the GIFI from the perspective of the cooperating units



873. According to the surveys distributed in 2021 among the cooperating units, including the law enforcement agencies and supervisory authorities, the cooperation with GIFI was most frequently assessed as good or very good (approx. 95.0% of all surveys in which this question was answered). The comments enclosed to some assessment included however the annotations on the absence of relevant trainings covering the control of the obligated institutions and insufficient information flow.

874. The international cooperation of the GIFI, in particular exchange of information with its foreign counterparts, is relatively good. The existing regulations impose no restrictions on the GIFI in terms of the scope and type of provided data.[442] The responses to the requests for information from abroad are also provided in a relatively short period of time (in 2020 within approx. 6 days on average[443], a half of responses was sent within 3 days [444]). The exchange of information takes place by means of 2 dedicated ICT systems i.e. ESW (in the scope of cooperation with the non-EU FIUs) and FIU.NET (in the case of cooperation with the EU FIUs).

[440] Estimated on the basis of cases completed in this year. In 2021, the average was approx. 14 days, while in 2020 – approx. 12 days.
[441] That is in the case of approx. 55.8% of cases (in 2021 approx. 47.8% of cases, while in 2020 – approx. 49.9% of cases).
[442] It should be noted that the war in Ukraine stifled the cooperation with Russia and Belarus. This was affected by among others the statements and decisions of FATF and of the Council of Europe.
[443] Estimated on the basis of cases completed in this year. In 2021, the average was of approx. 11 days, similarly as in 2020.
[444] That is in the case of approx. 51.3% of cases (in 2021 approx. 29.4% of cases, while in 2020 – approx. 27.7% of cases)

875. On the basis of information referred to above on the operation of the Polish Financial Intelligence Unit, the level of vulnerability in this area can be assessed as low.[445]

876. There are 2 bodies in Poland, which analyse and discuss the issues related to anti-money laundering and counter-terrorism financing as well as the predicate offences for money laundering. The first one is the Financial Security Committee operating under the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. Another one is the Interministerial Team for Terrorist Threats. Their members include the GIFI and the representatives of the law enforcement agencies as well as of the other public administration authorities. The meetings of these bodies are held on a regular basis.

877. With regard to the exchange of information at the national level, a key role is played by the National Centre of Criminal Information, which collects the criminal information and via which obtaining additional information from the other entities obliged to submit information to the National Centre of Criminal Information is possible.

878. As indicated above, the law enforcement agencies have relevant knowledge on the risk of money laundering and terrorism financing. They are relatively well capable of countering money laundering and terrorism financing (assessed on the basis of the existing powers as well as human, technical and financial resources).

879. Law enforcement agencies – within the survey referred to above distributed in 2021 among the cooperating units including the law enforcement – assessed the foreign cooperation their counterparts from the EU and non-EU countries and with the international authorities and organisations as good as very good in the area of anti-money laundering or counter-terrorism financing (the responses provided by the law enforcement agencies are rather not limited in terms of scope and type of data, while their large part uses the electronic communications channels for quick and safe exchange of information with the foreign counterparts – in particular in cooperation within the EU).

880. According to information referring to the operation of the law enforcement agencies, the level of vulnerability can be assessed as medium.

881. The justice authorities have adequate awareness of the risk of money laundering and terrorism financing. The National School of Judiciary and Public Prosecution (Polish: Krajowa Szkoła Sądownictwa i Prokuratury) organises many trainings enabling widening of knowledge by the judges, judicial staff and the prosecutors, including on the predicate offences for money laundering (e.g. in 2020 – in the scope of such thematic areas as: "Tax offences related to VAT and excise tax", "Crime in the area of trading in historical objects", "Methodology of corruption proceedings", "Cross-border organised crime with particular focus on the methods of seizure and recovery of the proceeds of crime". In addition, it also conducts the trainings referring directly to money laundering and terrorist financing (in 2022 the training entitled "Preparatory proceedings in the money laundering and terrorism financing" was organised, while the training entitled "Anti-money laundering and counter-terrorism financing from the perspective of the registration procedure") is planned for 2023.[446]

[445] It should be pointed out that the evaluation report of Moneyval carried out in 2021, the assessment of implementation of the FATF Recommendation 29 referring to the operation of the financial intelligence unit scored high rates – at the "compliant" level.

[446] https://www.kssip.gov.pl/, access on 06.03.2023

882. According to data on the penal proceedings brought before the regional and district courts in the criminal cases under Article 299 of the Penal Code, there were 316 penal proceedings initiated in 2022 i.e. by approx. 5.3% more than in 2021 and by approx. 18.8% more than in 2020. The number of penal penalties completed in 2022 was accordingly higher i.e. 261 (which is by approx. 15.5% than in 2021 and by approx. 76.4% more than in 2020). Although the number of finally convicted persons in 2022 was slightly lower than in 2021 (236 compared to 295), it was still definitely higher than in 2020 (186 persons and 1 collective entity finally convicted). The number of persons convicted in the 1st instance has increased on a regular basis – in 2022 it was 547 persons i.e. by 28.4% more than in 2021 and by 102.6% more than in 2020.

883. According to the above-mentioned data, the criminal cases under Article 299 of the Penal Code have been increasingly more frequently decided before the common courts and the increasing number of persons has been convicted. This confirms growing knowledge and awareness of the representatives of justice authorities in the field of the crime of money laundering.

884. One should also note the average duration of the penal proceedings before the court. According to data provided by the Ministry of Justice, it extended between 2019 and 2021 and was – in the case of an average duration of the proceeding from the date of the first registration in the district court to the date of final sentence in the district court of 1st instance – 6,0 months, while in the case of an average duration of the proceeding from the date of first registration in the district court to the date of final sentence in the regional court of 2nd instance, after the extension recorded in 2020, in 2021 it has remained at more or less the same level (8.7 months). In 2022, an onset of a downward trend in the average duration of the proceedings in all the a/m categories is observable. It is also linked with the decrease in the number of cases noticeable in this year, which were continued in the district courts and courts of appeal in the following period (170,750 and 7,241 respectively, i.e. less than in 2021 – by approx. 6.6% for the district courts and by approx. 1.5% for the regional courts, as well as less than in 2020 – by approx. 7.2% for the district courts and approx. 0.3% for the regional courts). This can be associated with catching-up past backlogs which appeared after the outbreak of pandemic in 2020.

885. The average duration of the proceeding from the first date of registration in the regional court to the date of the final sentence in the court of appeal of 2nd instance looks a bit different. In this case, its continuous increase has been observed since 2020, however in 2020 it was relatively low compared to the previous year.

Table 36. Average duration of the proceeding (in months) in penal proceedings before the court (rep. K) in 2019-2022.

Years	From the date of first registration in the district court to the date of final sentence in the district court of 1st instance	From the date of first registration in the regional court to the date of final sentence in the regional court of 1st instance	From the date of first registration in the district court to the date of final sentence in the regional court of 2nd instance	From the date of first registration in the regional court to the date of final sentence in the court of appeal of 2nd instance
2019	5.1	7.6	18.1	21.8
2020	5.8	8.7	19.7	24.0
2021	6.0	8.7	19.9	24.9

2022	5.8	8.6	19.8	25.0

886. In context of information described above it should be noted that according to data collected by the European Commission on the average duration of penal proceedings before the courts in the money laundering cases in the 1st instance for 2021 in the EU countries, in vast majority of the other EU states this duration exceeded 8.5 months (in 13 of 19 countries, from which data were obtained).

887. On the basis of information referred to above concerning the activities of the justice authorities, the level of vulnerability can be assessed as between low and medium.

888. The existing regulations in the area of anti-money laundering and counter-terrorism financing correspond to the risk of money laundering and terrorism financing and to the EU regulations and FATF recommendations to a very large extent, There are however the areas – in particular these identified in the report on the latest evaluation carried out by the MONEYVAL Committee evaluators and listed in chapter 7.2. – which require improvements (thus in this scope the level of vulnerability can be assessed as medium).

889. To sum up, the level of vulnerability for money laundering (as well as terrorist financing)[447] in the scope of inherent risk can be assessed as medium.

Level of consequences

890. According to data published in the 2022 statistical yearbook, the number of crimes ascertained by the Police and prosecutor's office in completed preparatory proceedings in 2021 increased by approx. 7.0% compared to 2020. A significant increase was observed in the number of offences against property, which was of approx. 12.9%, and the number of fraud offences surged by approx. 29.1%.[448] It should be noted that the total number of crimes ascertained by the Police and prosecutor's office in completed preparatory proceedings in 2020 was lower by approx. 3.9% compared to 2019 data (decrease recorded among others in the offences against property set out in Articles 278-295 of the Penal Code [approx. 2.1%] or offences against business activity under Article 296c-309 of the Penal Code [approx. 17.1%] and offences against money and securities trading under Articles 310-315 of the Penal Code [approx. 21.8%]).[449]

891. According to the Police data, the total detectability of offences was 71.2% in 2021, which translates into a relatively small decrease compared to 2018-2020 data (when it exceeded 73%). In the first place, the detectability of economic crimes decreased (constituting approx. 27.4% of all offences ascertained by the Police in 2021). In 2021, it amounted to 74.5% (i.e. by 11.6 percentage points less compared to 2018), while the detectability of corruption offences has remained more or less at a similar level since 2010 (i.e. above 99%). In 2021, it was 99.3% (99.7% in 2019-2020, 99.5% in 2018). Increased detectability was recorded in offences under the *Act on counteracting drug addiction* and so called criminal offences (referring among others to robberies, coercions and thefts with assault, as well as burglaries o thefts of property or cars).

[447] According to the adopted methodology presented in Annex 1, the level of vulnerability in the area of terrorism financing versus the inherent risk assessment should be based on the same components as in the case of estimating the level of vulnerability in the scope of money laundering for the purposes of inherent risk assessment.
[448] Based on data from: Statistical Yearbook of the Republic of Poland 2022, Statistics Poland, Warsaw 2022, pp. 148-150, at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/.
[449] Based on data from: Statistical Yearbook of the Republic of Poland 2021, Statistics Poland, Warsaw 2021, pp. 149-151, at: https://stat.gov.pl/obszary-tematyczne/roczniki-statystyczne/.

In the former case, it increased by 0.9 percentage point (from 96.3% in 2018 to 97.2% in 2021), in the latter – by 5.8 percentage points (from 39.3% in 2018 to 45.1% in 2021).[450]

892. According to the Public Opinion Research Center (CBOS) surveys of May 2022, approx. 83% of the respondents declared that living in Poland is safe (i.e. by 1 percentage point more compared to the survey of May 2021), while 13% of the respondents declared the opposite. In addition, as many as 96% of the respondents stated that their neighbourhood is a safe and calm place (the opposite opinion was provided by only 4% of the respondents).[451] A majority of the respondents, i.e. 58% (increase by 1 percentage point compared to data from the previous year survey) felt unthreatened by crime (i.e. "had no feeling of personal threat and becoming a victim of any crime"), while approx. 4% of the respondents declared high concerns of becoming a victim of a crime and approx. 36% declared moderate concerns in this field.[452]

893. According to the analysis by the Institute of Economic Forecasting and Analysis entitled *Szara Strefa 2022* (2022 Shadow Economy), the decrease in the share of shadow economy in the Polish economy progressing by 2019 has been contained after the outbreak of the COVID-19 pandemic, and with regard to the extending military conflict in Ukraine, this share may additionally increase up to 19.4% (the preliminary estimations for 2022 indicate the level of 18.9%).[453] The recent analysis presents the forecast of this share for 2023 at the level of 19.6%.[454] Although the key reasons behind development of this phenomenon included no elements directly linked with criminal activity, the authors stated with reference to the previous years that: "2021 was the year of further intensification of the shadow economy development factors, which appeared in 2020. In addition, such phenomena as illegal traffic with products and services closely related to the coronavirus pandemic (illicit trading in vaccines, vaccination certificates, etc.) have been recorded."

894. There are no data indicating the aggregate impact of illegal activity on the public sector income value. According to information, in the course of the operational and intelligence activities within the competences of the Central Anti-Corruption Bureau, the potential losses in property of the State Treasury in the following amounts were revealed: approx. PLN 5.88 billion in 2019, approx. PLN 4.60 billion in 2020 and approx. PLN 4.57 billion in 2021.[455] (during the controls and the analytical and informational activities, the officers of the control department of the Central Anti-Corruption Bureau revealed also the loss in property of the State Treasury or exposure to such loss in the amount of PLN 290 million in 2019, PLN 244 million in 2020, PLN 286 million in 2021[456] and in 2022 – PLN 236 million[457]).

895. There are no uniform and complete data on the costs of operation of the public and private sector entities related to ensuring the security of their operation and the society. Based

[450] https://statystyka.policja.pl/st/przestepstwa-ogolem/121940,Przestepstwa-ogolem.html, access on 24.02.2023.
[451] Poczucie bezpieczeństwa i zagrożenia przestępczością, Komunikat z badań, nr 76/2022, Public Opinion Research Center (CBOS), June 2022, pp. 1-3.
[452] Ibidem, p. 4.
[453] J. Fundowicz, K. Łapiński, B. Wyżnikiewicz, D. Wyżnikiewicz, Szara strefa 2022, Institute of Economic Forecasting and Analysis Scientific Foundation, Warsaw, March 2022, p. 17, at: https://www.ipag.org.pl/Content/Uploaded/files/IPAG_Szara_Strefa_2022_final.pdf.
[454] J. Fundowicz, K. Łapiński, B. Wyżnikiewicz, Szara strefa 2023, Institute of Economic Forecasting and Analysis Scientific foundation, Warsaw, March 2023, p. 9, at: https://www.ipag.org.pl/Content/Uploaded/files/IPAG_Szara_Strefa_2023.pdf
[455] Information on the operational results of the Central Anti-Corruption Bureau in 2021, p. 10 (at: https://www.cba.gov.pl/pl/o-nas/informacja-o-wynikach).
[456] Ibidem, p. 20.
[457] Information on the operational results of the Central Anti-Corruption Bureau in 2022., p. 15 (at: https://www.cba.gov.pl/pl/o-nas/informacja-o-wynikach).

however on sparse information pertaining to this area, it should be assumed that these costs continue to grow, both with regard to the increasing inflation and development of the new tools necessary to ensure greater transparency in economic trading, more effective analytical activities and penal proceedings and increase in the labour costs in certain entities and institutions (including with regard to covering the new categories of the obligated institutions with the anti-money laundering and terrorism financing regulations).

896. No collected information indicates the presence of political consequences. In the 2021 evaluation report of the Moneyval Committee certain deficiencies were identified and Poland was obliged to present the progress report on the implementation of the provided recommendations. It was not stated however that the reliability of Poland on the international forum has decreased with regard to the level of crime or operation of the anti-money laundering and counter-terrorism financing system.

897. To sum up, with a view to the upward trend of the identified crimes and the identified decrease in the detectability level, the areas of deficiencies of the AML/CFT system identified in the report from the latest evaluation carried out by the evaluators of the MONEYVAL Committee as well as vicinity of the military conflict in Ukraine – the level of consequences for money laundering in the scope of inherent risk should be estimated as between medium and significant (factor of 2.5).

Estimation of inherent risk

898. According to the methodology presented in Annex 1, the estimate of inherent risk for money laundering should be calculated using the formula: $R_{rp}=60\%*P_{prp}+40\%*K_{rp}$[458], provided that $P_{prp}= 40\%*Z_{rp}+60\%*P_{rp}$[459]. Based on the latter formula, the level of probability of money laundering versus inherent risk assessment i.e. P_{prp} is 2.4, which means that is at the medium level. According to the former formula, the risk of money laundering in the scope of inherent risk is 2.44 and is at the medium level.

8.1.2. Estimation of residual risk

899. Under the sectoral assessment carried out on the basis of the available data, the levels of risk for 14 areas were estimated. When performing the assessment, the money laundering risk scenarios for the selected products and services in the particular areas, for which the levels of threat and vulnerability were presented separately, were taken into account. The results of this analysis were presented in the table below (risk for money laundering was calculated on the basis of the averaged levels of threat and vulnerability assigned to the particular products/services as well as taking into account the fixed factor of the level of consequences estimated for the overall money laundering risk).

[458] Where: R_{rp} – level of "inherent risk", P_{prp} – level of probability of money laundering versus "inherent risk" assessment, K_{rp} – level of consequences of money laundering versus "inherent risk" assessment.
[459] Where: Z_{rp} – level of threat of money laundering versus "inherent risk" assessment, P_{rp} – level of vulnerability of money laundering versus "inherent risk" assessment.

Table 37. Money laundering risk levels for particular areas

Area	Averaged vulnerability	Averaged threat	Estimated level of risk
1. Area – banking	2.75	2.75	2.65
2. Area – payment services (offered by entities other than banks)	3	2.33	2.64
3. Area – insurances	2	2	2.20
4. Area – other financial institutions	2	2.2	2.25
5. Area – foreign currency exchange	2.33	3.33	2.64
6. Area – virtual currencies	3	3	2.80
7. Area - telecommunications services linked with mobile payments	4	2	2.92
8. Area – physical cross-border transportation of assets	3.5	3.5	3.10
9. Area – gambling	2	2.75	2.38
10. Area – non-profit organisations	3	3	2.80
11. Area – crowdfunding	4	2	2.92
12. Area - trade in high-value goods	3	2.5	2.68
13. Area – business activity (in general)	2.5	4	2.86
14. Area - real estates	2.0	3.0	2.44

900. According to the above estimates, none of the areas was estimated at the level of very high risk. High risk was assigned to the following areas (i.e. these with the level of risk >= 2.6 – according to the adopted methodology):

- banking,
- payment services (offered by entities other than banks),
- foreign currency exchange,
- virtual currencies,
- physical cross-border transportation of assets,
- telecommunications services linked with mobile payments,
- crowdfunding,
- trade in high-value goods,
- business activity (in general),

- non-profit organisations.

901. The medium level of risk was assigned to the remaining areas.

902. The estimate of money laundering risk in the area of residual risk, calculated on the basis of risk levels of the particular areas is approx. 2.66 and is at the high level.

8.1.3. Estimation of overall risk

903. Estimation of overall risk of money laundering consists in correlating the estimate of residual risk with the estimate of inherent risk using the formula: R_O=33.3%*R_P+66.7%*R_S[460]. On this basis, the estimate of overall risk of money laundering is approx. 2.59 and is at the medium level.

8.2. TERRORISM FINANCING RISK ASSESSMENT

8.2.1. Estimation of inherent risk

Level of threat

904. Although Poland is identified as the country of very low level of terrorism threat (e.g. the think tank – the Institute for Economics&Peace ranked Poland 93rd in the Global Terrorism Index 2023, with 0 rating[461]), this does not mean that the threat of terrorism financing must be also assessed at the same level. The practice of terrorism financing is linked not only with financing of the potential activities taken by the terrorist at the territory of the country, but features a more global nature and may be associated with collection in Poland of assets for the purposes of various persons and groups suspected of terrorism and operating in the other countries.

905. According to data provided by the Ministry of Justice for the purposes of the GIFI reports on the implementation of the *Act on counteracting money laundering and financing of terrorism*:

(1) In 2020, the common courts initiated 1 penal proceeding with regard to the offence under Article 165a of the Penal Code and completed one penal proceeding under this Article. In effect of the proceeding with the offence under Article 165a of the Penal Code ended in 2020 1 person was convicted in the 1st instance, while in 2020 no persons finally convicted for terrorism financing were recorded;

(2) In 2021-2022 the common courts initiated no penal proceedings with regard to the offence under 165a of the Penal Code and completed not a one penal proceeding under this Article. In 2021, with regard to the offence under Article 165a of the Penal Code, no persons were convicted, both in the 1st instance and finally.

906. Also information from the National Prosecutor's Office indicate a low number of penal proceedings with regard to the offence under Article 165a of the Penal Code (in 2020 1 such proceeding was initiated, in 2021 – 2, while in 2022 4 cases related to this crime were recorded). Statistical data on the total property seizures in the cases under Article 165a of the Penal Code for 2021 indicated the amount of PLN 2,151,137.58 (for 2020 PLN 1,240,321). These amounts

[460] Where: R_O – level of overall risk, R_P – level of inherent risk, R_S – level of residual risk.
[461] https://www.visionofhumanity.org/maps/global-terrorism-index/#/, access on 05.05.2023

of seizures fall within the range between 0.00005% and 0.000082% GDP, which would indicate a very high level of threat.

907. In its report on the supranational assessment of risk of money laundering and terrorist financing of 27 October 2022 determined to overall level of threat for terrorism financing for the UE.[462] The assessment identified, however, 43 products and services in 8 areas, which are potentially vulnerable to the risk of money laundering and/or terrorism financing and for which it determined the levels of threat and vulnerability (separately for money laundering and terrorism financing), provided that for the area "illegal transfers of funds – Hawala" no risk level of terrorism financing (and of money laundering) was determined due to absence of specific data for the threat assessment, including taking into account that: "…they are illegal within the EU. There is no specific vulnerability assessment for illegal services in the context of the supranational risk assessment report".[463] Based on the assessments of all the products/services described, it can be assumed that the terrorism financing risk in the EU is at a medium level.

908. With regard to preventing the events of terrorist nature in the Polish counter-terrorism system, the leading role in the identification of terrorism threats is played by the Head of the Internal Security Agency. He coordinates also the analytical and informational activities and exchange of information between the services in the scope of events of terrorist nature and is responsible for coordination of the operational and intelligence operations of the other sources in this area. Cooperation of the services and institutions of the Polish counter-terrorism system consists primarily in providing any and all information acquired by the system members, which fall within the catalogue of incidents and events subject to reporting to the Counter-Terrorist Centre of the Internal Security Agency. For example, in 2020-2022, the GIFI, when implementing the statutory tasks in the area of counter-terrorism financing, initiated 21 analytical proceedings referring to the transactions which could be potentially linked with terrorism financing. The basis for initiating the proceedings was information received from the cooperating units, the obligated institutions, as well as information or requests provided by the foreign financial intelligence units.

909. Based on the available data, it can be stated that there is information from at least several sources on the possible use of Poland for acquisition or transfer of assets for terrorist purposes, which would indicate the medium level of threat.

910. Under the *Act of 10 June 2016 on anti-terrorist activities, the President of the Council of Ministers, upon consulting the minister competent for interior and the Head of the Internal Security Agency, and in the urgent cases the minister competent for interior (who will immediately notify the President of the Council of Ministers), upon consulting the Head of the Internal Security Agency, may implement by means of an ordinance of the alert states, depending on the type of threat of a terrorist event. Since 2019, the alert levels have been implemented in Poland in the following cases*:

[462] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, European Commission, Brussels, 27.10.2022, at: https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en.
[463] Ibidem, p. 84.

(1) Ministerial meeting on the security in the Middle East held in Warsaw – the first alert state ALFA and second alert level BRAVO CRP were implemented in the capital city of Warsaw between 11 and 15 February 2019;

(2) Elections to the European Parliament in 2019 – the second alert level BRAVO-CRP was implemented throughout the territory of the Republic of Poland between 23 and 27 May 2019;

(3) Celebrations of the 80th anniversary of the WW II outbreak – the first alert level ALFA and the first alert level ALFA-CRP were implemented throughout the territory of the Republic of Poland between 28 August 2019 and 3 September 2019;

(4) Elections to the Sejm and Senate in 2019 – the second alert level BRAVO-CRP was implemented throughout the territory of the Republic of Poland between 10 and 14 October 2019;

(5) Celebrations commemorating the 75th anniversary of the liberation of the nazi concentration and extermination camp Auschwitz-Birkenau – the second alert level BRAVO was implemented at the territory of the Lesser Poland Voivodeship, the first alert level ALFA was implemented throughout the remaining territory of the Republic of Poland and the first alert level ALFA-CRP was implemented throughout the entire territory of the Republic of Poland. The alert levels were in force between 23 and 29 January 2020;

(6) Elections of the President of the Republic of Poland in 2020 – the second alert level BRAVO-CRP was implemented throughout the territory of the Republic of Poland between 26 and 29 June 2020 and between 10 and 13 July 2020;

(7) UN Digital Summit - IGF 2021 (the UN Internet Governance Forum) in Katowice – the first alert level ALFA-CRP was implemented throughout the territory of the Republic of Poland between 5 and 10 December 2021;

(8) With regard to the potential risk for the ICT systems security linked with the identified threats resulting from tense situation in the region (military attack in Ukraine and hybrid actions by Russia and Belarus):

- the first alert level ALFA-CRP was implemented throughout the territory of the Republic of Poland between 18 and 23 January 2022 and between 15 and 21 February 2022,
- the third alert level CHARLIE-CRP implemented throughout the territory of the Republic of Poland between 21 February 2022 (since 9:00 PM) and 31 May 2023.

(9) With regard to the increased and forecasted threat of a terrorist event resulting from mass inflow of the Ukrainian refugees to the territory of the Republic of Poland:

- the second alert level (BRAVO) was implemented at the territory of the Lublin and Podkarpackie Voivodeship between 28 February and 15 April 2022,
- the second alert level (BRAVO) was implemented throughout the territory of the Republic of Poland between 16 April 2022 and 31 May 2023,
- for the Polish energy infrastructure outside the boundaries of the Republic of Poland the second alert level (BRAVO) was implemented between 6 October 2022 and 31 May 2023.

911. In the scope referred to above, the level of threat can be assessed as very high.

912. Considering the above, it should be stated that the level of threat of terrorism financing is high.

Level of vulnerability

913. Pursuant to the adopted methodology, the level of vulnerability is the same as the level estimated for the vulnerability to money laundering for inherent risk i.e. at the medium level. The justification is presented in sub-chapter 8.1.1.

Level of consequences

914. No available information indicate a significant level of terrorist activity in the country or of financing of terrorist activity. No increase in the criminal activity, from which the funds allocated to terrorist activity could origin, was identified. One should, however, take into account the conclusions contained in the report from the latest evaluation performed by the evaluators of the MONEYVAL Committee along with the listed areas of the AML/CFT system deficiencies, as well as the vicinity of the military conflict in Ukraine and the associated implications. In this context the level of consequences can be estimated as low with an upward trend (low consequences to moderate).

915. The remaining components (specified in Table 12 in Annex 1 to this document), necessary to estimate the level of consequences in the area of terrorism financing for the purposes of inherent risk assessment were already discussed as the basis for estimating the consequences in the area of money laundering for the inherent risk assessment (see sub-chapter 8.1.1.).

916. Considering the above, the consequences in the area of terrorism financing for the inherent risk can be estimated at the level between low and moderate (i.e. determining it as low consequences to moderate – factor of 1.5).

Estimation of inherent risk

917. According to the methodology presented in Annex 1, the estimate of inherent risk fo terrorism financing should be calculated using the formula: $R_{rp\_ft}=60\%*P_{prp\_ft}+40\%*K_{rp\_ft}$[464], provided that $P_{prp\_ft}= 40\%*Z_{rp\_ft}+60\%*P_{rp\_ft}$[465]. Based on the latter formula, the level of probability of terrorism financing versus inherent risk assessment i.e. P_{prp_ft} is 2.4, which means that it is at the medium level. According to the former formula, the risk of terrorism financing for inherent risk is approx. 2.04 and its level is medium.

8.2.2. Estimation of residual risk

Level of threat

918. Under the sectoral assessment carried out on the basis of the available data, the levels of risk for 14 areas were estimated. When performing the assessment, the terrorism financing risk scenarios for the selected products and services in the particular areas, for which the levels of threat and vulnerability were presented separately, were taken into account. The results of this analysis were presented in the table below (risk for terrorism financing was calculated on the

[464] Where: R_{rp_ft} – level of „inherent risk", P_{prp_ft} – level of probability of terrorism financing versus the "inherent risk" assessment, K_{rp_ft} – level of consequences of terrorism financing versus the "inherent risk" assessment

[465] Where: Z_{rp_ft} – level of threat of terrorism financing versus the "inherent risk" assessment, P_{rp_Ft} – level of vulnerability of terrorism financing versus the "inherent risk" assessment.

basis of the averaged levels of threat and vulnerability assigned to the particular products/services as well as taking into account the fixed factor of the level of consequences estimated for the overall terrorism financing risk)

Table 38. Terrorism financing risk levels for particular areas

Area	Averaged vulnerability	Averaged threat	Estimated level of risk
1. Area – banking	2.75	3	2.31
2. Area – payment services (offered by entities other than banks)	3.33	3.67	2.68
3. Area – insurances	3	1	1.92
4. Area – other financial institutions	2	1	1.56
5. Area – foreign currency exchange	2	2	1.80
6. Area – virtual currencies	3	3	2.40
7. Area - telecommunications services linked with mobile payments	4	1	2.28
8. Area – physical cross-border transportation of assets	4	3.5	2.88
9. Area – gambling	2	1	1.56
10. Area – non-profit organisations	3	2	2.16
11. Area – crowdfunding	4	2	2.52
12. Area - trade in high-value goods	3	1.5	2.04
13. Area – business activity (in general)	2	2	1.80
14. Area - real estates	2	3	2.04

919. According to the above estimates, none of the areas was estimated at the level of very high risk. High risk (i.e. level of risk >= 2.6 – according to the adopted methodology) was assigned to the physical cross-border transportation of assets and payment services (offered by entities other than banks).

920. The medium level of risk was assigned to all remaining areas excluding other financial institutions and gambling, which are covered by low level of risk.

921. The estimate of the risk of terrorism financing for residual risk, calculated on the basis of the levels of risk of the particular areas, is approx. 2.14 and is at the medium level.

8.2.3. Estimation of overall risk

922. Estimation of the overall risk of terrorism financing consists in correlating the estimate of residual risk with the estimate of inherent risk using the following formula: R_{O_ft}=33.3%*R_{P_ft}+66.7%*R_{S_ft}[466]. On this basis, the estimate of the overall risk of terrorism financing is approx. 2.11 and is at the medium level.

[466] Where: R_{O_ft} – level of overall risk, R_{P_ft} – level of inherent risk, R_{S_ft} – level of residual risk.

9. CONCLUSIONS

923. Due to the dynamic development of financial services and products, variability of distribution channels, introduction of new technologies, and volatility of the levels of threats and susceptibility to money laundering or terrorism financing, the Polish national AML/CFT system is verified, updated and improved in order to optimise its operation. To this end, legal provisions and procedures are improved, relevant training for employees of the FIU, cooperating units and obligated institutions is provided, and electronic documents and ICT systems that increase the efficiency of this system are used. An efficient Polish AML/CFT system also means effective supervision (especially financial) and control, as well as enforcement of legal provisions. This is the complementarity of the activities carried out by the FIU with those carried out by law enforcement agencies, authorities supervising obligated institutions, courts and other competent state authorities. It is also the adequate application of customer due diligence measures as well as modification and development of risk management methods in obligated institutions that take into account changes in the economic environment as well as apply regulatory requirements and good market practice made available by the competent authorities.

924. A risk-based approach as the basis for managing the anti-money laundering process requires proactive actions from obligated institutions. An approach based on the formal application of applicable legal provisions and only passive enforcement of regulatory requirements and standards is no longer sufficient. A risk-based approach requires the identification, assessment and understanding of the ML/FT risks to which obligated institutions are exposed. There is also a clear obligation for these institutions to implement relevant actions to mitigate these risks. Obligated institutions should use all available risk management methods, including risk prevention, risk transfer to other entities, risk acceptance, abandoning certain activities, and risk monitoring.

925. The application of relevant mitigating measures in the AML/CFT system, resulting, among others, from the findings of the National Risk Assessment of Money Laundering and Financing of Terrorism, leads to increasingly effective operation of the authorities participating in this system and more efficient prosecution of ML/FT offences. The use of mitigating measures in the AML/CFT system prevents criminals from benefiting from crime or makes it much more difficult for them, while facilitating the identification of the directions of development of organised crime in Poland (especially money laundering and terrorism as well as its financing). It may also make it easier to recognise the methods currently used by criminals.

926. The most well-known measures mitigating the risk of money laundering and terrorism financing, that are also most common in the Polish AML/CFT system, include customer due diligence measures applied by obligated institutions. These measures are specified in the *Act on counteracting money laundering and financing of terrorism* and include, among others, identification of the customer and verification of its identity; identification of the beneficial

owner and taking reasonable steps in order to verify its identity, determine its structure of ownership and control – in the case of a customer that is a legal person, an organisational unit without legal personality or a trust; assessment of business relationships, and, as appropriate, obtaining information on their purpose and intended nature; ongoing monitoring of the customer's business relationships. The monitoring of the customer's business relationships consists in the analysis of transactions carried out as part of business relationships to ensure that these transactions are consistent with the obligated institution's knowledge of a given customer, the type and scope of its business, and with the ML/FT related to this customer. Where relevant, such monitoring also includes examining the source of the assets held by the customer and ensuring that the documents, data or information regarding business relationships are updated on an ongoing basis. Obligated institutions must intensify their analyses and activities aimed at the adequate application of the aforementioned mitigating measures as well as updating these activities in the context of changing technologies, products, amended legislation and geographical factors.

927. Moreover, obligated institutions, especially given the armed conflict in the immediate vicinity of Poland's borders, must optimise the application of customer due diligence regarding verification of the identity of the customer, the person authorised to act on its behalf and its beneficial owner, as well as deepen the analysis of business relationships and their monitoring in the event of suspected money laundering or terrorism financing and conducting an investigation into such cases by competent authorities. What is to mitigate the risk in this case is the legal obligation imposed on the obligated institution to report to the GIFI cases of suspected money laundering or terrorism financing, as well as effective training for employees carried out by the GIFI and other cooperating units and obligated institutions. Constant updating of training content will significantly increase awareness and understanding of obligations in the field of counteracting money laundering and terrorism financing.

928. The money laundering risk assessment estimates for particular areas carried out herein showed that the following areas were classified as high risk ones (this was the highest calculated level, because no area was found to be related to very high risk): banking, payment services (offered by entities other than banks), foreign currency exchange, virtual currencies, physical cross-border transportation of assets; telecommunications services linked with mobile payments; crowdfunding; business activities (general), trade in high-value goods, and non-profit organisations. The aforementioned areas showed a money laundering risk level of >= 2.6 – in accordance with the methodology adopted in the document. The terrorism financing risk assessment estimates for particular areas showed that the following areas were classified as high risk ones (this was the highest calculated level, because no area was found to be related to very high risk): physical cross-border transportation of assets and payment services (offered by entities other than banks).

The aforementioned money laundering and terrorism financing areas require special attention. Measures mitigating money laundering and terrorism financing risks, undertaken both at the legislative and practical level, should apply in particular to these areas. The need to apply mitigating measures in the field of counteracting money laundering and terrorism financing applies both to the GIFI as well as obligated institutions and cooperating units being part of the AML/CFT system. This will enable adaptation to the changing reality in terms of money laundering and terrorism financing. Intensified analyses of statistical data obtained from obligated institutions will allow for a better assessment of ML/FT risks both in individual

entities and in the entire sector. This will also enable the GIFI to improve the process of analysing and planning control activities. Based on, among others, the foregoing, the GIFI will enhance the effectiveness of planning control activities in particular obligated institutions. It will also enable more effective tracking of new ML/FT trends and methods, as well as their proper understanding and management, which affects the effectiveness of undertaken control activities. More efficient activities of the GIFI will allow obligated institutions to streamline the preparation of the risk assessment matrix, take specific risk assessment criteria – including the specific characteristics of a given obligated institution into account, assign an adequate weight to each criterion, indicate the correlation between risk factors and the risk assessment findings, and recommend the use of adequate mitigating measures, specific for a given obligated institution (that can actually mitigate the risk).

929. Legislative mitigating measures are used with respect to risks relating to particular financial services/products generating a relatively high risk of money laundering or terrorism financing. The most important legislative mitigating measures include the issuance and entry into force of regulations to the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*. Since the publication of the first National Risk Assessment of money laundering and financing of terrorism, the provisions regarding the Central Register of Beneficial Owners and the list of domestic public positions and functions classified as politically exposed persons have come into force, and National Revenue Administration bodies have been designated to perform the tasks of the authority competent to maintain the register of virtual currency service providers, as well as to perform the tasks of the authority competent to maintain the register of trust and company service providers. During training courses conducted by the GIFI (as well as other institutions), the theoretical and practical aspects of counteracting money laundering and terrorism financing are explored, which prevents criminals from concealing their identity in a complicated corporate structure or makes it much more difficult for them, as well as increases the control of information regarding customers of obligated institutions. Moreover, in June 2021, the provisions of *Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005* (OJ L 284/6, 12.11.2018) and implementing regulations thereto establishing templates for certain forms as well as technical rules for the effective exchange of information under this Regulation entered into force. This Regulation limits the risks related to the flow of assets across the EU borders, due to the introduced system for control of cash entering and leaving the EU, exchange of information between competent authorities, including FIUs, registration of information regarding the declarant, the owner, the sender and the recipient or intended recipient of the cash, including the name and surname, contact details, and the nature and the amount or value of the cash, its economic provenance and its intended use. Moreover, FIUs have been granted access to the customs information system established by Council Regulation (EC) No 515/97. However, the provisions in question should be supplemented at the national level with provisions introducing a real penalty for failure to report cross-border transportation of currency. At the same time, the mechanism for detaining assets transported contrary to the regulations should be improved to include possible confiscation of cash.

930. The need to regulate and organise the cryptocurrency market has been addressed by the adoption by the EU Parliament and the Council of the *Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937* (called MiCA). This Regulation comprehensively regulates the operation of crypto-assets in trading, harmonises the digital market for financial

services, makes cross-border services available to European consumers, and introduces a pan-European licencing system for activities based on virtual values. It also requires crypto-asset companies to identify their customers. The adoption and entry into force in 2023 of the provisions of the *Act on the Financial Information System*, by which the legislator resolved to set up a Financial Information System (SInF) for collecting, processing and sharing information on open and closed accounts is yet another important mitigating measure. For the aforementioned regulations to be properly applied, obligated institutions are required to provide relevant training to their employees, covering also the practical aspects of their implementation, also in terms of the proper and timely updating of information in internal data files, as well as to develop relevant instructions. Strong awareness of obligated institutions' employees of exposure to money laundering and terrorism financing offences will enable adequate risk assessment and the application of adequate customer due diligence measures.

931. The activities provided for by the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism*, aimed at systemic mitigation of ML/FT risks, include the development of information on areas and sectors particularly vulnerable to ML/FT risks, made available by the GIFI by 15 November each year. This information is provided to the entities referred to in Article 130(2) of the aforementioned Act. Moreover, in order to systemically mitigate the risk of money laundering and terrorism financing, the GIFI develops instructions on monitoring compliance with the provisions of the aforementioned Act and makes them available to those entities. Both information on areas and sectors particularly vulnerable to the risk of money laundering or terrorist financing, as well as guidance on monitoring compliance with the provisions of the aforementioned Act, concern primarily those areas in which the ML/FT risk assessment estimates for particular areas showed a high risk level. In areas vulnerable to high or medium ML/FT risks, the GIFI provides information on identified threats and vulnerabilities. These concern abuses, system vulnerabilities, suspicious activities of types of entities and the products and services used by them that pose an ML/FT threat, identified in specific areas, to which risk mitigating measures should be applied. Entities referred to in Article 130(2) of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* use information on areas and sectors particularly vulnerable to risk and guidance on monitoring compliance with the provisions of the aforementioned Act, in accordance with the specific characteristics of the activities carried out by controlled obligated institutions.

932. Risks generated by capital and financial market entities are primarily addressed with the key measure mitigating the identified risk, i.e. supervision exercised over these obligated institutions by the Polish Financial Supervision Authority. Market regulation is the key mitigating measure in this respect, and the activities and initiatives of the Polish Financial Supervision Authority significantly reduce the scale of the ML/FT risks generated by the market.

933. Due to the ML/FT risks generated by products and services that are particularly vulnerable to being misused in order to commit fraud and market abuse or transferring/storing proceeds of crime, it is crucial to use mitigating measures adapted to the specific characteristics of such products and services. In particular, in the case of products such as collect services offered by the banking sector for financial intermediaries, that are a high-risk area because this type of product makes it difficult to identify the payer and the actual recipient of the transaction,

it is crucial to properly identify the needs of the customer using such services. Obligated institutions should, among other things, verify the validity of launching a collect service for customers whose business scale and nature do not substantiate the need to launch such service. Obligated institutions should also pay particular attention to electronic money transfer/money order services, as they are considered to be highly vulnerable to the risk of money laundering and financing of terrorism. The need to apply mitigating measures was identified also in the case of safe deposit services due to the limited ability of obligated institutions to monitor the content of safe deposit boxes, as well as other products and services that by their nature favour anonymity, e.g. bearer instruments or products and services characterised by extraordinary complexity with no obvious economic purpose. The risk generated by safe deposit boxes will be considerably mitigated be the Financial Information System (SInF), to which data on safe deposit boxes is to be reported starting from the third quarter of 2023.

934. As regards the activities of capital market entities, it is necessary to mitigate the risk generated by products and services consisting in: raising funds from a closed group of natural persons and business entities and investing the thus raised funds; raising funds from many people on account of alleged investments on the Forex market – the aggrieved parties can make payments to the accounts of business entities registered for "straw men" – the thus raised funds are then transferred to foreign entities. An increased level of risk has also been identified in the case of raising and investing funds from natural persons from another country or other countries on account of alleged capital investments and investing in closed-end investment funds – the holder of the certificates holds them anonymously and can trade them uncontrolled by tax authorities and capital market supervision authorities. What poses a threat is that closed-end investment funds can be used to purchase shares and real estate, and the income generated by such entities (with certain exceptions) is not taxed. The presented risks should be mitigated by the obligated institutions offering the services and products concerned, as well as by those obligated institutions whose customers use these products and services. The main mitigating measures in this respect should consist in the adequate application of customer due diligence, with particular emphasis on verifying the source of the customer's assets and obtaining information on the purpose and intended nature of the customer's activities that arouse the obligated institution's suspicion. The risk related to the operation of closed-end investment funds should be mitigated by the adequate application of customer due diligence measures by obligated institutions setting up and managing funds, taking the specific characteristics of the offered products and the customers acceding to investment funds into account. Risks related to improper performance of their obligations in this area by obligated institutions should be mitigated in particular by the supervisory activities of the Polish Financial Supervision Authority and the GIFI's inspections.

935. The noticeable level of money laundering risk in the case of payment institutions entails the need to apply adequately adapted mitigating measures due to a measurable increase in the number of natural persons acting as the so-called partners of other obligated institutions dealing with cryptocurrency exchange, making it difficult to identify the source of the funds. There was also a small number of notifications submitted by entities engaged in online foreign currency exchange and payment service providers, which, given their increasing activity, raises questions about the reliability of the performance of their statutory obligations by the obligated institutions concerned. As part of the application of mitigating measures, market supervisory institutions should conduct a detailed analysis of payment institutions' activities in opening

numerous payment accounts for foreign entities, which may be related to the intensification of opening accounts based on fictitious documents. At the same time, obligated institutions should strengthen activities related to the identification and verification of the customer's identity in order to mitigate the risk related to the use of fictitious or stolen documents. The activities of small payment institutions and payment service offices should be subject to enhanced supervision, in particular in terms of identifying difficulties with the actual monitoring of customer transactions. As part of the application of mitigating measures, enhanced supervision by the competent authorities is also recommended in the case of the activities of foreign payment institutions whose accounts are kept by domestic banks, as there is a risk that domestic banks do not have sufficient information on the foreign entities to which they provide their services. The competent supervisory authorities should apply mitigating measures to payment institutions in the case of cascade structures, where payment institutions serve other payment institutions. In such cases, identification of the actual payer and payee is difficult or impossible. In this respect, the risk related to the activities of entities subject to supervision outside Poland may be mitigated by developing efficient exchange of information between domestic and foreign supervisory authorities. Special supervision should also be extended over those institutions that are registered in Poland but owned by foreigners, as well as those institutions that, apart from having an account/accounts in Poland, do not seem to have any other links with Poland. The risk related to the operation of some payment institutions may be mitigated by selection and adequate application of supervisory measures to institutions that are personally linked to other payment institutions (where a given person establishes subsequent payment institutions – usually payment service offices), as well as institutions providing services to which they are not entitled or exceeding the turnover limits for a given institution category.

936. Mitigating measures should also be applied to reduce the likelihood of using cryptocurrency exchanges/trading facilities operating as dealers in exchange operated by financial institutions for money laundering and terrorism financing, as well as using virtual assets to transfer value from illicit sources. Mitigating measures are also required where business relationships are established at a distance without the physical presence of the customer in the obligated institution's premises and where the obligated institution conducts business from a virtual office.

937. Obligated institutions should also pay attention to the fact that increased money laundering risk is generated also by entrusting the implementation of customer due diligence measures to third parties that are not prepared for this task, with the high turnover of employees operationally involved in the performance of AML/CFT duties in the obligated institution. The low level of technical/technological knowledge in obligated institutions is also indicated (lack of adequate tools/software or a low technical level of system solutions). Placing special emphasis by obligated institutions on counteracting the aforementioned phenomena is a *sine qua non* for mitigating the risk of using the obligated institutions concerned for money laundering or terrorism financing.

938. In order to reduce the likelihood of entities conducting business activities being used for money laundering or terrorism financing, it is reasonable for obligated institutions to take risk-limiting actions by applying mitigating measures when establishing business relationships with persons who do not actually have any assets and are only used as "straw men" by other people/entities to conceal the identity of those who actually own these assets. The key to risk

mitigation is the proper application of customer due diligence measures by obligated institutions, with particular emphasis on updating information regarding the customer, having adequate knowledge of the customer, including the assessment of its business relationships, or taking steps to verify the source of its assets. Likewise, obligated institutions must take adequate measures to mitigate the risk of money laundering and terrorism financing when establishing business relationships with entities engaged in crowdfunding (assessed as an area with a high ML/FT risk), as crowdfunding facilitates the concealment of the source of funds and generates ML/FT risks for obligated institutions, especially in cases of an improperly conducted KYC process, which results in the financial institution having insufficient knowledge of the entity is serves. Mitigating the risk related to crowdfunding should primarily consist in adequate verification of the sources of assets and in a transaction analysis carried out as part of the ongoing monitoring of business relationships. In order to mitigate risks related to crowdfunding it may be necessary to request customers of obligated institutions to provide detailed information regarding their transactions, in particular where payments made for a given entity are characterised by unusual circumstances, such as a large number of payments in a short time, payments of significant unit value, or a large number of payments from non-residents or from foreign jurisdictions.

939. Obligated institutions must apply risk mitigating measures when establishing business relationships with customers who are non-residents/foreigners who do not have clearly identified personal/economic links with the territory of Poland, in particular those who carry out transactions only or mainly with other non-residents/foreigners. Obligated institutions should also deepen their analyses where a threat in the form of the obligated institution continuing business relationships despite being unable to apply customer due diligence measures to the customer/trading partner is identified. Obligated institutions must avoid re-establishing business relationships with an institutional customer's representatives and proxies who have previously been identified by a given obligated institution as persons who may be involved in money laundering and terrorism financing.

940. As part of the application of mitigating measures to reduce the likelihood of obligated institutions being used to money laundering and terrorism financing, these institutions must provide relevant training to for their employees and improve internal instructions, as in some cases, obligated institutions failed to identify whether the beneficial owner or representative of the customer was a politically exposed person. Deficiencies in the identification by obligated institutions of the customer's beneficial owners who are citizens of or live in high ML/FT risk countries, as well as the failure to verify the customer's beneficial owners on sanctions lists, should also be eliminated. When taking mitigating actions, obligated institutions must also aim to eliminate cases of the obligated institution continuing business relationships with the customer, despite negative information regarding its activities.

941. In areas of activities particularly vulnerable to ML/FT risks, that are subject to control by the National Revenue Administration, mitigating measures should be applied to carousel transactions and chain transactions involving missing traders. In order to reduce the likelihood of entities conducting business activities being used for money laundering or terrorism financing, the National Revenue Administration bodies should improve the effectiveness of activities aimed at counteracting: issuing VAT invoices documenting transactions that did not actually take place; using invoices that do not document actual economic events; crediting

personal accounts with receivables for: supply of goods/provision of services, or issuing dummy invoices; failure to declare intra-Community supplies of goods/intra-Community acquisitions of goods by an eligible entity (international buffer), even though the entity's accounts are credited with cash; failure to declare the full amount of turnover; trading in Voice over IP (VoIP) signals. The National Revenue Administration bodies must apply mitigating measures also in the case of: fraud related to trade in guarantees of origin (GO); illegal trade in excise goods, such as alcohol, tobacco products and dried tobacco; activities involving games of chance, betting, card games and games on gaming machines; trade in expensive alcohol and biocides, where the entity organising illegal trade in denatured alcohol most often registers business activities for "straw men"; obtaining illicit income from the sale of documents used as evidence in obtaining Schengen visas. Mitigating measures may, in particular, consist in intensifying control activities or developing analytical functions related to the adequate selection of persons and entities involved in illegal activities. In order to mitigate threats identified at the system level the National Revenue Administration bodies have been authorised to access information collected in the Financial Information System (SInF), which will facilitate the implementation of the National Revenue Administration's tasks. The National Revenue Administration bodies must apply measures mitigating ML/FT risks also to:

(a) bond issues by capital companies that are legal entities listed in Article 2(1)(a) of the Act of 15 January 2015 on bonds (Journal of Laws of 2020, item 2244), addressed only to members of a criminal group;

(b) increasing the company's share capital in exchange for debt, addressed only to partners who are members of a criminal group;

(c) activities of companies providing maintenance services, IT services, accounting services, HR and payroll services, specialist transport services (this type of activity involves groups obtaining funds from illegal trade in fuel and gambling);

(d) broadly understood trade in works of art and antiques in the context of domestic and cross-border trade.

942. As regards the areas of activities highly vulnerable to ML/FT risks, the use of measures mitigating these risks is of particular importance in the case of foundations (applies to the non-profit organisation sector, where money laundering risk has been estimated at a high level) established pursuant to the *Act of 6 April 1984 on foundations*. Obligated institutions should conduct in-depth analyses of transactions underlying the operation of these organisations, related, in particular, to the following ML/FT risk elements: numerous sources of funding, with a simultaneous lack of transparency and information on the ultimate use of funds; the foundation's links with politically exposed persons (PEP) and entities conducting business activities; conducting by the foundation business activities that are inconsistent with its statute; using methods of raising funds that facilitate the concealment of their sources and the identity of actual donors (e.g. fundraisers). Mitigating measures should also include counteracting threats related to possible links of non-profit organisations (foundations, associations) with extremist organisations or their representatives.

943. In connection with the analysis of financial flows (regarding data on above-threshold transactions [> equivalent of EUR 15,000] made in 2020-2022) between Poland and countries applying harmful tax competition, particularly diligent application of customer due diligence

measures by obligated institutions is required. The total amounts of transfers sent from Poland to countries applying harmful tax competition, as stated in Annex No. 3, indicate that these countries would be a major area of Polish foreign trade in terms of financial turnover. This is the case where the value of transfers leaving Poland is much higher than that of transfers coming to Poland. The necessity for obligated institutions to extend special supervision over transactions with countries applying harmful tax competition is due to the fact that transfers involving the countries concerned may include a number of such transactions that are related to concealing proceeds from illegal sources, tax avoidance or the need to legalise income obtained contrary to law. Obligated institutions should pay particular attention to the accuracy of monitoring the customer's business relationships, examining the source of the assets held by the customer, identifying the beneficial owner, and taking reasonable steps to verify its identity.

944. In their risk analyses, obligated institutions should take into account the entry into force of the *Act of 26 January 2023 on family foundations* (Journal of Laws of 2023, item 326) on 22 May 2023, that regulates the organisation and operation of family foundations (including the rights and obligations of founders and beneficiaries), and analyse the possible use of their products and services – in the context of this Act – for illegal purposes. This is even more important because in Poland, there are almost 830,000 family businesses, 57% of which plan succession by 2028.[467] Identification and assessment by obligated institutions of ML/FT risks, taking into account risk factors related to customers, countries or geographical areas, products, services, transactions or their supply channels must be confronted with the assumed Act objectives regarding effective, multi-generational company succession, building strong family brands, keeping capital by the family and protecting it against fragmentation. An accurate assessment of the ML/FT risks generated by the obligated institutions concerned will inform the decision whether to apply mitigating measures to the products and services offered by obligated institutions.

945. Several general mitigating measures have been formulated with respect to obligated institutions, whose application will reduce the institution's exposure to the risk of money laundering and terrorism financing. Such mitigating measures include:

- obligated institutions maintaining bank or payment accounts should pay particular attention to transfers of funds to jurisdictions characterised by higher ML/FT risk. In particular, they should pay attention to regular transfers of funds with an enigmatic transfer title, or repeated transfers of funds to a given jurisdiction, in the absence of economic substantiation for this type of transfers. Obliged institutions should consider requesting the customer to provide details of the source of the transferred assets, as well as documents substantiating a given transaction,
- obligated institutions should pay attention to the reason for carrying out a given transaction, in particular to confirm that it is consistent with their knowledge of the customer. In particular, attention should be paid to recurring patterns of transactions between related entities,
- obligated institutions should pay attention to the entity's address, in particular with regard to its registration in a virtual office. In the case of such entities, it is important

[467] Data of the Family Business Institute – source: Gazeta Prawna, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8720117,ustawa-o-fundacji-rodzinnej.html

to determine whether the account is used to carry out transactions typical of an entity conducting actual business activity, such as utility bills or salary costs,

- as for the threats related to the risk of money laundering through cash deposits/withdrawals, obligated institutions should consider the advisability of introducing limits on cash deposits/withdrawals for particular categories of customers, established based on the information provided by the obligated institution about the customer. Exceeding the daily and monthly limit should be possible after the customer contacts the obligated institution and substantiates the need to carry out a transaction inconsistent with its declaration,
- obligated institutions should train employees who apply customer due diligence measures, taking specialist knowledge in identifying counterfeit documents into account. Obligated institutions establishing business relationships at a distance should also select measures for the identification and verification of the customer's identity, enabling real verification of the characteristics of the document confirming the customer's identity.
- risk mitigation with respect to products such as collect accounts should be combined with special verification of the customer's needs in this area, as well as with increased monitoring of the use of the service,
- obligated institutions should consider verification of the source of the customer's assets not only when obtaining high-value incoming transfers, but also in the case of, for example, loan repayments, in particular in the case of early repayment of the loan where according to the information on the customer's income it is not possible to raise funds to overpay the loan in the declared amount,
- all activities related to a value transfer should involve the adaptation of customer due diligence measures to the risk level in the country of origin of the funds/country of destination of the funds,
- if the customer of the obligated institution uses solutions enabling payments via payment terminals or applications for making payments, the obligated institution should take into account circumstances indicating a disproportionately high value of the transaction in relation to the customer's business profile, or in relation to previously collected information about the customer.

LIST OF ANNEXES