

REPORT
of the General Inspector of Financial Information
on the implementation *of the provisions of the Act of*
1 March 2018
on counteracting money laundering
and financing of terrorism
in 2024

Warsaw, March 2025

TABLE OF CONTENTS

1. INTRODUCTION	7
2. KEY INFORMATION ON THE NATIONAL ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING SYSTEM	9
2.1. NATIONAL ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING SYSTEM	9
2.2. INFORMATION ON CATEGORIES OF OBLIGATED INSTITUTIONS	15
2.2.1. ENTITIES OPERATING IN THE FINANCIAL MARKET	15
2.2.2. OTHER CATEGORIES OF OBLIGATED INSTITUTIONS	26
3. INFORMATION ON DATA SUBMITTED TO THE GIF	37
3.2. INFORMATION ON ABOVE THRESHOLD TRANSACTIONS	41
4. ANALYSES	44
4.1. COUNTERACTING MONEY LAUNDERING	44
4.1.1. ANALYTICAL PROCEEDINGS AND THEIR EFFECTS	44
4.1.2. EXAMPLES OF ANALYSIS DIRECTIONS (INCLUDING SANITISED CASES)	49
4.2. COUNTERACTING THE FINANCING OF TERRORISM	60
5. INSPECTIONS	63
5.1. INFORMATION FROM WHISTLEBLOWERS	63
5.2. INSPECTIONS PERFORMED BY THE GIF	63
5.3. INSPECTIONS CARRIED OUT BY SUPERVISORY INSTITUTIONS	65
5.4. ADMINISTRATIVE PROCEEDINGS REGARDING IMPOSITION OF ADMINISTRATIVE SANCTIONS	65
6. NATIONAL COOPERATION	67
6.1. EXCHANGE OF INFORMATION WITH DOMESTIC ENTITIES	67
6.1.1. COOPERATION WITH ORGANISATIONAL UNITS OF THE PROSECUTOR'S OFFICE AND COURTS	67
6.1.2. COOPERATION WITH THE NATIONAL REVENUE ADMINISTRATION BODIES	69
6.1.3. COOPERATION WITH BODIES SUBORDINATED TO THE MINISTER OF THE INTERIOR	70
6.1.4. COOPERATION WITH STATE SECURITY SERVICES	70
6.1.5. COOPERATION WITH THE CENTRAL ANTI-CORRUPTION BUREAU	71
6.1.6. COOPERATION WITH OTHER AUTHORITIES	71
6.1.7. COOPERATION WITH THE NATIONAL CENTRE FOR CRIMINAL INFORMATION	71
6.2. FEEDBACK	72
6.2.1. NATIONAL REVENUE ADMINISTRATION BODIES	73
6.2.2. THE POLICE	75
6.2.3. OTHER AUTHORITIES	78
6.3. DATA CONCERNING CRIMINAL PROCEEDINGS	80
6.4. TRAINING ACTIVITY	81
7. INTERNATIONAL COOPERATION	84
7.1. COOPERATION WITH THE EUROPEAN COMMISSION	84
7.1.1. EXPERT GROUP ON MONEY LAUNDERING AND TERRORIST FINANCING	84
7.1.2. EU-FIU PLATFORM	85
7.2. COOPERATION WITH THE COUNCIL OF THE EU	86

7.3 MONEYVAL COMMITTEE	86
7.4. CONFERENCE OF THE STATES PARTIES TO THE WARSAW CONVENTION	89
7.5. EGMONT GROUP	91
7.6. FINANCIAL ACTION TASK FORCE	92
7.7. EURASIAN GROUP ON COMBATING MONEY LAUNDERING	95
7.8. COUNTER ISIS FINANCE GROUP	95
7.9 BILATERAL COOPERATION	96
7.9.1. BASIS OF INFORMATION EXCHANGE WITH FOREIGN FIUS	96
7.9.2 EXCHANGE OF INFORMATION WITH FOREIGN FINANCIAL INTELLIGENCE UNITS	96
7.10. OTHER INTERNATIONAL INITIATIVES	104
7.10.1. THE PROJECT "STRENGTHENING THE RISK ASSESSMENT MECHANISMS AND THE STRATEGIC ANALYSIS FUNCTION OF THE POLISH FINANCIAL INTELLIGENCE UNIT"	104
7.10.2. WORKSHOP FOR UKRAINIAN ADMINISTRATION REPRESENTATIVES CO-HOSTED WITH THE OSCE	106
7.10.3. FIU REGIONAL WORKSHOPS UNDER THE POLISH PRESIDENCY OF THE V4	106
7.10.4. STUDY VISITS	106
7.10.5. OTHER INITIATIVES	107
7.10.6. AEOI REVIEW	108
7.10.7. CHOOSING THE SEAT AND APPOINTING THE CHAIR OF THE AMLA	109
7.11. INTERNATIONAL COOPERATION IN THE AREA OF AML/CFT SUPERVISION AND CONTROL	109
7.11.1 COOPERATION WITH THE EUROPEAN BANKING AUTHORITY (EBA)	109
7.11.2 COOPERATION WITH COMPETENT SUPERVISORY AUTHORITIES IN PARTICULAR COUNTRIES	111
8. APPLICATION OF SPECIFIC RESTRICTIVE MEASURES	112
9. FINANCIAL SECURITY COMMITTEE	114
10. WORK ON UPDATING THE STRATEGY FOR COUNTERACTING MONEY LAUNDERING AND FINANCING OF TERRORISM	116
11. LEGISLATIVE ACTIVITY	118

Abbreviations and acronyms:

ABW	Internal Security Agency
AML/CFT	anti-money laundering and countering the financing of terrorism
AML/CFT/CFP	anti-money laundering, counter-terrorism financing and countering the financing of proliferation
OPS	Office of Payment Services
CAT	ABW Anti-Terrorist Centre
CBA	Central Anti-Corruption Bureau
CBŚP	Central Bureau of Investigation of the Police
CBZC	Central Bureau for Combating Cybercrime
CIFG	Counter-ISIL Finance Group
COP	Conference of the Parties to the CETS 198, i.e. the Conference of the States Parties to the Warsaw Convention (the body established under Article 48 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 - CETS 198, that stipulates the creation of a monitoring mechanism to ensure the application of its provisions)
Journal of Laws	Journal of Laws of the Republic of Poland
OJ EU	Official Journal of the European Union (OJ of the EU)
EAG	ang. The Eurasian Group on Combating Money Laundering and Financing of Terrorism (organisation established in 2004 as a FATF-style regional body and a FATF associate member)
EBA	European Banking Authority
EGMLTF	Expert Group on Money Laundering and Terrorist Financing, operating at the European Commission
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force (established in 1989 during the G-7 Summit in Paris, dealing with the analysis and assessment of threats related to money laundering and financing of terrorism, in particular in the context of 40 recommendations it has issued, defining the international standards concerning the counteracting of money laundering and financing of terrorism and their proliferation)
GIFI	General Inspector of Financial Information
GPW S.A.	Giełda Papierów Wartościowych w Warszawie S.A. (Warsaw Stock Exchange)
GUS	Statistics Poland
IAS	Revenue Administration Regional Office

OI	obligated institution referred to in Article 2(1) of the <i>Act of 1 March 2018 on counteracting money laundering and financing of terrorism</i> (consolidated text, Journal of Laws of 2023, item 1124, as amended)
ISIS	Islamic State of Iraq and Sham
FIU	Financial Intelligence Unit (in accordance with FATF Recommendation 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”)
CU	cooperating unit referred to in Article 2(2)(8) of the <i>Act of 1 March 2018 on counteracting money laundering and financing of terrorism</i>
KAS	National Revenue Administration
KCIK	National Centre of Criminal Information
KDPW S.A.	Krajowy Depozyt Papierów Wartościowych S.A. (National Depository of Securities)
EC	European Commission
KGP	Police Headquarters
DPI	domestic payment institution
KNF	Polish Financial Supervision Authority
UKNF	Office of the Polish Financial Supervision Authority
ML/TF	money laundering / terrorist financing
SPI	Small Payment Institutions
MONEYVAL	also referred to as the MONEYVAL Committee – Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (the body of the Council of Europe established in 1997 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 associate member)
ITTT	Inter-Ministerial Team for Terrorist Threats (established by <i>Ordinance 162 of the Prime Minister of 25 October 2006</i> as an auxiliary body of the Council of Ministers to ensure cooperation of the governmental administration in detecting, preventing and counteracting terrorism)
NBP	National Bank of Poland
OSCE	<i>Organization for Security and Co-operation in Europe</i>
PKD	Polish Classification of Activities
SAR	Suspicious Activity Report
BG	Border Guard

SKOK	Cooperative Savings and Credit Union
SKW	Military Counter-Intelligence Service
SNRA	Supranational Risk Assessment (for the area of money laundering and terrorist financing)
TSI	Technical Support Instrument of the European Commission
EU	European Union

1. INTRODUCTION

Countering money laundering and financing of terrorism is a multifaceted task, carried out both domestically and in international cooperation fora (including in the field of information exchange), within the public and private sectors. It is carried out not only by the General Inspector of Financial Information (GIFI), but also by other entities operating within the scope of the national system of counteracting the above-mentioned crimes, as defined in the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* (Journal of Laws of 2023, item 1124, as amended), hereinafter referred to as the AML/CFT Act, as cooperating units and obligated institutions. Therefore, the information presented in this report relates not only to the results of the GIFI's work, but also of those entities.

In 2024, a relatively large increase in notifications of suspicious activity and transactions received by the GIFI – so-called Suspicious Activity Reports (SARs) – was noted, i.e. by approximately 71.3% compared to the 2023 data. At the same time, it should be emphasised that although the number of notifications received from both cooperating units (up by approx. 35.6%) and obligated institutions (up by approx. 74.3%) has increased, in absolute numbers the increase is mainly noticeable in the latter category. Compared to the 2021 data, the number of SARs from obligated institutions doubled (i.e. there was an increase of approx. 113.6%). The above upward trend can also be seen at the beginning of the current year.

A similar increase in the information received was also noticeable in the field of international cooperation. Foreign Financial Intelligence Units submitted to the GIFI - in addition to their requests for information or responses to such requests sent by the GIFI - additional information concerning unusual or suspicious transactions or other activities involving Polish entities or assets transferred to/from the territory of Poland. In 2024, the GIFI received approx. 67.6% more of these than in 2023, and compared to the 2021 data, the number was more than two and a half times higher (i.e. by approx. 161.5%).

The large increase in incoming information to be analysed, as indicated above, also requires correspondingly larger workload on the part of the GIFI, which is a challenge given the limited size of its resources, in particular human resources. Nevertheless, within the framework of its activities in 2024, the GIFI, among others, initiated approx. 38.4 % more analytical investigations than in the previous year and forwarded 757 notifications (in total: main and supplementary) to the prosecutor's office, as well as 532 notifications to cooperating units (in particular to the KAS and law enforcement agencies), i.e. approx. 3.0% and approx. 23.1% more than in 2023, respectively. The answer to these challenges is the execution of a project aimed at the implementation of goAML software in the Polish FIU and the structured transfer of information within the national anti-money laundering and counter-terrorist financing system.

The implementation of the task of counteracting money laundering and terrorist financing is also related to the adaptation of regulations and operating procedures to the constantly emerging new challenges in this field, as well as to the accordingly changing international standards and regulations. The changes in the domestic anti-money laundering and counter-terrorist financing system that have taken place in recent years have been noted by the MONEYVAL Committee, which at the end of last year accepted Poland's request to upgrade its assessment of the

implementation of two Financial Action Task Force (FATF) recommendations, i.e. No. 1 and No. 33, to the *largely compliant* (LC) level.

In conclusion, it is worth highlighting the important role played by the GIFI and the Department of Financial Information of the Ministry of Finance in the global network against money laundering and terrorist financing. This importance materialises, among other things, through the international recognition of our staff. Particular mention should be made here of Ms Elżbieta Franków-Jaśkiewicz (Deputy Director of the above-mentioned Department), who was elected as the new Chair of the Egmont Group at its plenary meeting in June 2024. At the same time, the Council of Europe honoured her professionalism and expertise as part of the project "75 Women in 75 Years of Council of Europe History" in connection with her activity in the global network for combating money laundering and terrorist financing.

2. KEY INFORMATION ON THE NATIONAL ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING SYSTEM

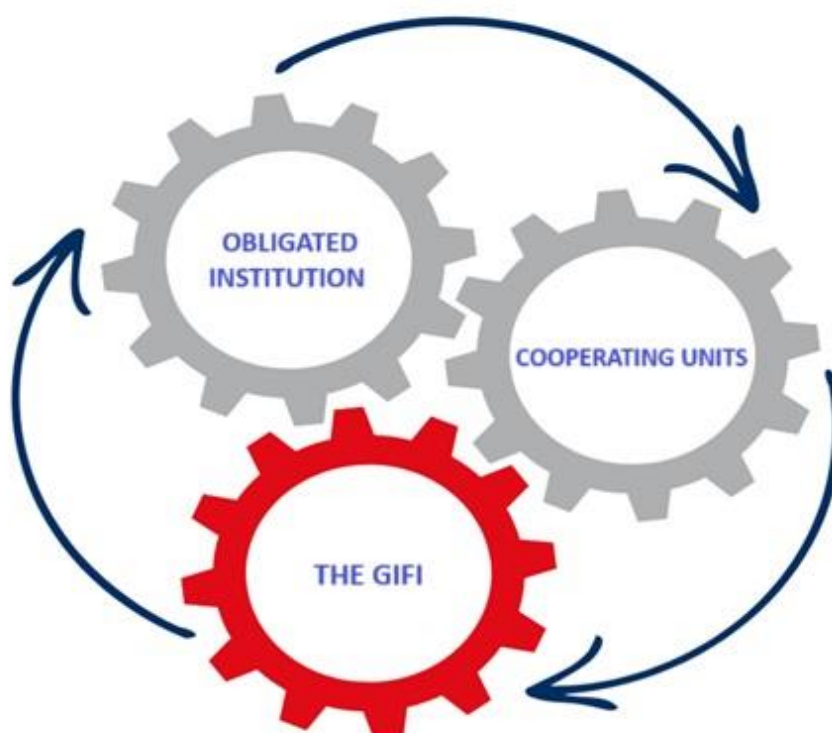
2.1. NATIONAL ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING SYSTEM

The Polish anti-money laundering and counter-terrorist financing system (hereinafter referred to as "*AML/CFT system*") is based on domestic and EU legal regulations. The key legal act that defines the principles of its operation is the *AML/CFT Act*, which indicates measures to counter these procedures, specifies the powers of cooperating bodies and units and defines the obligations of obligated institutions under the *AML/CFT system*.

The Polish Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) system consists of:

- The General Inspector of Financial Information (GIFI);
- obligated institutions (OI);
- cooperating units (CU).

Figure 1 – Diagram of the national AML/CFT system



Obligated Institutions, the GIFI and cooperating units interact and influence each other. Activities carried out by obligated institutions directly influence the GIFI's initiatives, which, in turn, shape the operation of cooperating units, in particular law enforcement agencies and

supervisory authorities. At the same time, the effectiveness of the work of cooperating units is important for the activities carried out by the GIFI, which is then reflected in the activities of obligated institutions. As a result, the *AML/CFT* system operates on the principle of "communicating vessels", in which the quality and effectiveness of each component affects the performance of the others and the efficiency of the entire system.

Pursuant to the *AML/CFT Act*, the government administration bodies responsible for counteracting money laundering and terrorism financing are the minister competent for public finance (acting as the supreme financial information authority) and the GIFI. Given the scope and nature of its responsibilities, the GIFI, as the central element of the *AML/CFT* system, has the greatest impact on its functioning. It is worth emphasising that this system is also largely shaped by the legislative process, which includes the implementation of solutions provided for in relevant EU directives into Polish law.

In accordance with the provisions of the *AML/CFT Act*, the GIFI performs its tasks through a separate organisational unit within the structure of the Ministry of Finance – the Department of Financial Information. Since 2017, employment in this Department has been systematically increasing, rising from 65 in 2017 to 122 in 2024. The organisational challenge is to ensure adequate office facilities for all employees.

Pursuant to Article 12(1) of the *AML/CFT Act*, the GIFI's tasks include taking action to counteract money laundering and terrorist financing, in particular:

- analysing information concerning assets suspected by the GIFI of being related to an offence of money laundering or terrorist financing;
- suspending transactions or blocking bank accounts;
- requesting submission of information on transactions and disclosure thereof;
- submitting information and documents substantiating the suspicion of committing an offence to competent authorities;
- exchanging information with cooperating units;
- developing the national assessment of the risk of money laundering and terrorist financing as well as strategies for counteracting such offences in cooperation with cooperating units and obligated institutions;
- exercising control over obligated institutions' compliance with the provisions on counteracting money laundering and terrorist financing¹;
- issuing decisions on entry into the list of persons and entities towards whom or which specific restrictive measures, involving the freezing of assets or refraining from making them available, in particular by refraining from granting loans, consumer loans or mortgage loans, refraining from making donations, and refraining from making payments for goods or services, are applied, or their delisting, and keeping this list;

¹ The GIFI also controls - with regard to obligated institutions referred to in the *AML/CFT Act* - compliance with the restrictive measures set out in the legal acts listed in Article 143c of the *Act on National Revenue Administration* (consolidated text, Journal of Laws of 2023, item 615, as amended).

- cooperation with competent authorities in other countries, as well as foreign institutions and international organisations dealing with counteracting money laundering or terrorist financing;
- exchange of information with foreign financial intelligence units, including running a contact point for the purposes of such exchange;
- imposing administrative penalties referred to in the *AML/CFT Act*;
- making knowledge and information relating to the provisions on counteracting money laundering and terrorist financing available 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 *AML/CFT Act*,
- initiating other activities to counteract money laundering and terrorist financing.

Obligated institutions are entities obliged to comply with the requirements and restrictions set out in the *AML/CFT Act*. The list of these institutions, set out in Art. 2(1) of this Act, includes as many as 30 different categories of entities from both the financial and non-financial sectors. It is an exhaustive list, which means that only the entities listed therein are obliged to fulfil the obligations arising from the *AML/CFT Act*.

The key obligation of obligated institutions is to identify and assess the risk of money laundering and terrorist financing in the context of business relationships with customers and occasional transactions carried out. On the basis of this assessment, these institutions implement adequate customer due diligence measures to obtain information about customers and the purpose of their activities. Where a money laundering or terrorist financing offence is suspected, obligated institutions are required to notify the GIFI immediately.

In addition, obligated institutions provide the GIFI with information on so-called above threshold transactions, the value of which exceeds EUR 15,000, which include:

- cash deposits and withdrawals;
- transfers of funds, including international transfers;
- foreign exchange purchase or sale transactions and the intermediation of such transactions;
- activities performed in the form of a notary deed, specified in the Act.

At the GIFI's request, obligated institutions are obliged to block accounts, suspend transactions as well as submit or make available any information and documents held. The account blockage or transaction suspension is based on a decision of a prosecutor.

In the context of counter-terrorism, obligated institutions also implement specific restrictive measures against persons and entities included on lists published by the minister competent for public finance in the Public Information Bulletin.

The GIFI is authorised to control compliance with obligations in the area of counteracting money laundering and terrorist financing. In addition, pursuant to Article 130(2) of the *AML/CFT Act*, control in this regard is also exercised by:

- President of the National Bank of Poland – over entities conducting currency exchange offices;
- the KNF – over institutions under its supervision;
- National Association of Cooperative Savings and Credit Unions – over cooperative savings and credit unions;
- Presidents of the courts of appeal – over notaries;
- Heads of the customs and tax control offices – over all obligated institutions;
- Province (voivodeship) or district (powiat) governors – over associations;
- Ministers or district (powiat) governors – over foundations.

Cooperating units include government administration bodies, local government bodies and other state organisational units, as well as the National Bank of Poland, the KNF and the Supreme Audit Office. They are obliged to promptly inform the GIFI of any suspicions of money laundering and terrorist financing offences and, at the GIFI's request, to provide information or documents within their statutory powers.

The GIFI analyses information contained in reports/notifications of suspected money laundering or terrorist financing using data provided by obligated institutions, cooperating units and foreign Financial Intelligence Units (FIUs). In the event of a reasonable suspicion that an offence has been committed, the GIFI forwards the notification to the competent prosecutor, who takes further action in cooperation with law enforcement agencies. The aim of these activities is to confirm information, collect evidence and prepare an indictment against the suspects.

Following the receipt of such notification, the prosecutor is obliged to notify the GIFI of:

- the issuance of a decision to block a bank account or suspend a transaction;
- suspension of proceedings;
- resumption of suspended proceedings;
- issuance of a decision to present charges.

In addition, prosecutors are required to provide the GIFI with information on the initiation of proceedings, presentation of charges, bringing of an indictment and account blockage or transaction suspension in other money laundering or terrorist financing cases.

The GIFI, at the written request of courts and prosecutors, makes collected information and documents available for the purposes of criminal proceedings. Furthermore, the institution shall provide financial information and financial analyses to other cooperating units, as defined in the *AML/CFT Act*, upon written and reasonable request. These entities include:

- the authorities indicated in Art. 105(1) 1 of the *AML/CFT Act*;
- Chairperson of the KNF;
- President of the National Bank of Poland;
- President of the Supreme Audit Office;

- national administrator in accordance with Commission Regulation (EU) No 389/2013²;
- minister competent for foreign affairs;
- the minister competent for public finance;
- head of the National Revenue Administration;
- director of the Revenue Administration Regional Office;
- head of the customs and tax control office.

When providing information to these entities, the GIFI determines the scope and purposes of its use in accordance with the applicable legal regulations.

In the event of a suspicion that a fiscal offence or an offence other than money laundering or terrorist financing has been committed, the GIFI shall forward information substantiating this suspicion to the competent law enforcement agencies, enabling them to take action in accordance with their powers. Moreover, the GIFI may also independently share information in its possession with law enforcement agencies in order to fulfil their statutory obligations. In the event of a suspected violation of regulations related to the operation of the financial market, the GIFI shall forward the relevant information to the Polish Financial Supervision Authority (KNF).

Due to the international nature of financial crime, the GIFI exchanges information with foreign FIUs. At the request of a foreign FIU, the GIFI may authorise the transfer of the information it makes available to other authorities or its use for purposes other than those specified in the tasks of FIUs. At the same time, the GIFI may also request permission from the foreign FIU to share the obtained information with courts, prosecutors, other cooperating units or to use it in other ways. In addition, pursuant to Article 113(4) of the *AML/CFT Act*, the GIFI has the right to request suspending a transaction or blocking an account at the request of a foreign FIU if the request contains sufficient justification for the suspicion of money laundering or terrorist financing.

The AML/CFT system is a complex structure, closely related to the provisions of the *AML/CFT Act* and national and EU regulations. Its functioning is crucial to various areas of the economy, including corporate activities, business relations and the execution of financial transactions. Countering these illegal practices is one of the fundamental tasks of the state, aiming to reduce crime and ensure financial security.

The effectiveness of this system largely depends on the reliability of obligated institutions in the implementation of their statutory obligations. Therefore, the *AML/CFT Act* provides for the possibility of imposing both administrative and criminal sanctions. Limiting these sanctions to the administrative aspect alone would be insufficient, which is why the criminalisation of money laundering is fully justified and is reflected in international agreements such as the

² Authority listed in Art. 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 EU L 122 of 03.05.2013, p. 1, as amended9).

Vienna Convention and the Palermo Convention, as well as in Recommendation No. 3 of the FATF.

The effectiveness of the AML/CFT system also relies on close cooperation between authorities and units at administrative and criminal levels. Proper coordination of these activities determines the efficiency of the entire system and contributes to increasing financial security and reducing the risk of economic crime.

The AML/CFT system operates on the basis of a risk-based approach. The introduction of the *AML/CFT Act* was intended to reduce the risk of the money laundering offences (Article 299 of the Penal Code), in line with FATF Recommendation No. 1. Based on its content, countries should identify, assess and understand the risks associated with money laundering and terrorist financing and take action, including establishing authorities or mechanisms to coordinate risk assessment. The measures applied under the system should be proportionate to the level of risk identified.

In order to ensure the effectiveness of the system, it is crucial to correctly identify risks and implement effective customer due diligence measures. The responsibility in this regard lies mainly with obligated institutions, which, by fulfilling their obligations in accordance with the *AML/CFT Act*, directly affect the effectiveness of the entire system. Another important aspect is the cooperation of supervisory authorities and cooperating units, whose task is to control obligated institutions and enforce compliance. The effectiveness of this process is also linked to the appropriate use of sanctions – both administrative and criminal – to induce obligated institutions to take appropriate action.

The system works as a complex mechanism in which each component must function efficiently to ensure its effectiveness. Timely exchange of information between the actors in the system is crucial, enabling the effective operation of supervisory authorities and the implementation of legal measures to ensure the effectiveness of the system.

Proper fulfilment of the obligations arising from the *AML/CFT Act* also requires a proper understanding of the provisions by obligated institutions. In this context, the GIFi plays an important role in ensuring the reliability of the activities undertaken by these institutions. The transfer of knowledge on AML/CFT is carried out through the organisation of training courses, the publication of announcements in the Public Information Bulletin and the development of a national risk assessment and strategy to counter these crimes in cooperation with other actors in the system.

A high level of regulatory awareness among obligated institutions translates into a more effective fulfilment of obligations, which ultimately strengthens the entire system. The GIFi's educational activities are also preventive in nature and may contribute to reducing the number of violations resulting in sanctions.

The shape and operation of the system is also directly influenced by the legislative process, which ensures its stability and adaptation to changing threats. International regulations, including EU directives and FATF recommendations, play a key role in its evolution and effectiveness. Thanks to international cooperation and the exchange of information with foreign FIUs, AML/CFT is becoming global in nature, allowing cross-border threats to be addressed more effectively.

2.2. INFORMATION ON CATEGORIES OF OBLIGATED INSTITUTIONS

Pursuant to the *AML/CFT Act*, there are 30 categories of obligated institutions³, including entities operating in the financial market and a numerous group of entities operating outside that market.

2.2.1. ENTITIES OPERATING IN THE FINANCIAL MARKET

The following description of categories of entities operating in the financial market has been drawn up based on information obtained by the GIFI under Article 14(4) of the *AML/CFT Act* from the Polish Financial Supervision Authority (KNF)⁴, the National Credit and Savings Union and the National Bank of Poland (NBP), concerning the entities supervised by them.

Banking sector

As at the end of December 2024,⁵ banking activities were carried out by 551 entities (29 commercial banks, 489 cooperative banks and 33 branches of credit institutions). The sector included a network of 9,700 facilities (4,943 branches, 2,211 affiliated branches and agencies and 2,551 representative offices). The banks employed 146,700 people. In the analysed period, the trend of reducing the banking network continued – banks continued efforts to increase the effectiveness of their operations by optimising the sales network.

Between 2023 and 2024, there was a slight increase in the number of banking sector employees, i.e. from 144,900 at the end of December 2023 to 146,700 at the end of December 2024.

The number of bank branches decreased between the end of 2023 and the end of 2024, i.e. from 4,948 to, 4,943 bank branches. The number of affiliated branches, agencies and other customer service facilities decreased from 2,342 (at the end of 2023) to 2,211 (at the end of 2024). The downward trend was recorded also in the number of representative offices, whose number decreased from 2,716 (as at the end of December 2023) to 2,551 (as at the end of December 2024).

The situation of the banking sector remained stable, despite the unstable geopolitical environment. In Q3 2024, a slight decrease in capital adequacy ratios was observed. Banks' own funds increased by 3.4% (y/y) from PLN 245 billion to PLN 253 billion at the end of Q3 2024. At the same time, the total amount of annualised risk exposure grew faster (by 7.1% to PLN 1,193 billion). The Tier 1 capital ratio was 20.0% and the total capital ratio was 21.3%. In the corresponding period of 2023, these ratios were 20.4% and 22.0%, respectively.

The current liquidity situation in commercial banks remained good. All commercial banks met the applicable LCR standard of 100%. As at the end of Q3 2024, the average LCR for the

³ As at 31 December 2024, 30 categories of obligated institutions were recorded in accordance with the *AML/CFT Act*, n 19.02.2025, the list of obligated institution categories was expanded to include credit servicers within the meaning of Article 3(1)(17) of the *Act of 20 December 2024 on credit servicers and credit purchasers* (Journal of Laws of 2025, item 146).

⁴ The information presented has been selected from a broader description of the financial market sectors provided by the KNF.

⁵ https://www.knf.gov.pl/?articleId=56224&p_id=18

commercial bank sector was 225%. The requirement regarding the Net Stable Funding Ratio (NSFR) was also met by all banks, and its average value in the period concerned was 163%.

The banking sector's net financial profit at the end of September 2024 was PLN 31.2 billion. The significant increase in the y/y profit was due to still high interest rates and, as a result, an increase in interest income, with a slight decrease in interest costs (interest costs decreased from PLN 53.9 billion to PLN 49.4 billion, while interest income increased from PLN 123.6 billion to PLN 128.4 billion).

As at the end of September 2024, five commercial banks reported a total loss of PLN 0.9 billion. These banks had an approx. 2.3% share in the assets of the commercial banking sector. Other banks in the sector reported a total profit of PLN 29.4 billion.

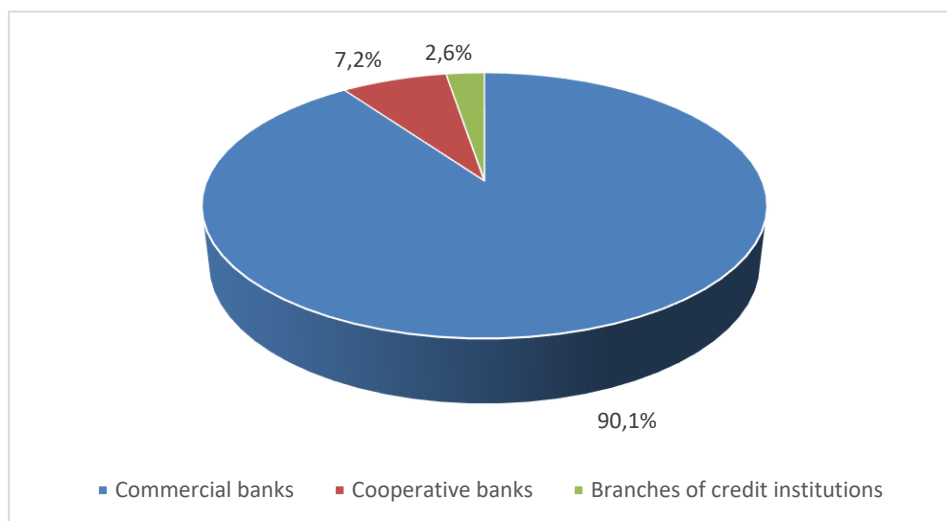
As regards branches of credit institutions, four entities, with a 9.2% share in the assets of all branches of credit institutions, reported a total loss of PLN 2.2 billion at the end of Q3 2024.

In the first three quarters of 2024, the banking environment was relatively favourable, especially due to the high level of interest rates, as well as, among others, low unemployment and rapidly growing nominal wages. For this reason, there was a significant improvement in the performance ratios compared to the previous year. As at the end of Q3 2024, ROE was 14.47% (+2.89 p.p. y/y); ROA was 1.23% (+0.32 p.p. y/y); R/I (provisions and write-offs to income ratio) remained stable: an increase from 19.35% to 19.65%. On the other hand, the banks regained the net interest margin (increase from 3.70% to 3.84% in the same period of the previous year) with strict cost control – the C/I ratio fell from 44.10% to 42.98%.

The main items in the asset structure of commercial and cooperative banks included loans and advances (50.7%, PLN 1,639.4 billion). Debt instruments accounted for 33.0% of the value of assets (PLN 1,066.7 billion), while the other receivables for 16.2% (PLN 524.4 billion). As for liabilities, the main items included deposits (PLN 2,291.6 billion, 70.9%), own issues (PLN 340.3 billion, 10.5%) and equity (PLN 274.9 billion, 8.5%).

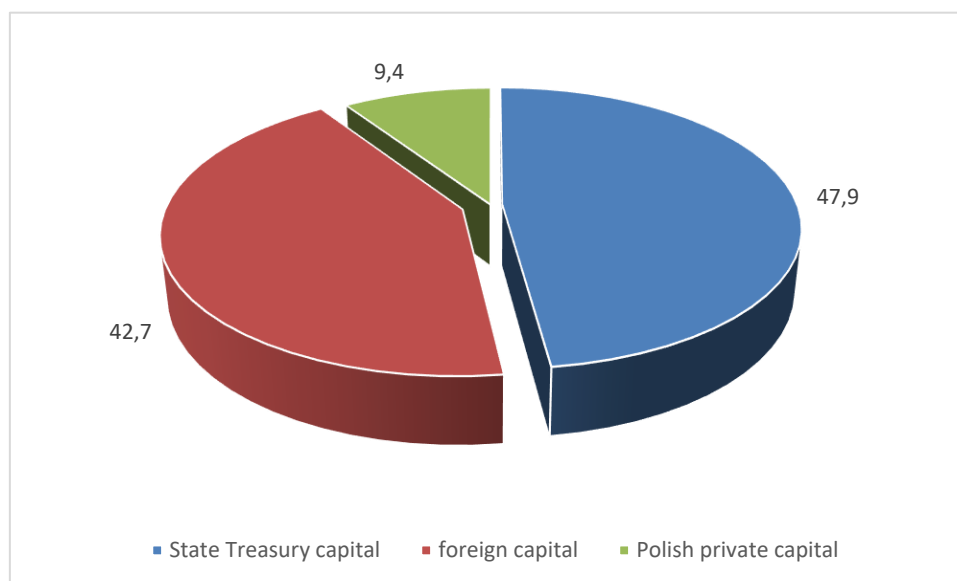
The stability of the banking sector is crucial to the stability of the entire financial system. As at the end of December 2024, the assets of the banking sector amounted to PLN 3,335 billion. Based on the available data, it is known that 90.1% of the banking sector's assets were managed by commercial banks, the share of cooperative banks in banking assets was 7.2% and that of branches of credit institutions was 2.6%.

Chart 1. Banking sector structure as at the end of December 2024 by percentage of particular entities in the total value of its assets



In the breakdown by dominant entity, as at the end of December this year, 47.9% of assets were controlled by the State Treasury, 42.7% by foreign capital and 9.4% by Polish private capital. The concentration of the banking sector at the end of 2024 was at a moderate level.

Chart 2. Percent structure of the banking sector by the origin of capital as at the end of December 2024



Current challenges/problems facing the banking sector include:

- 1) RRE (FX) loans – a portfolio of foreign currency mortgage loans generating systemic risk mainly due to the legal risk related to the high number of lawsuits filed by borrowers and the direction of court decisions regarding the shape of loan agreements.
- 2) Regional/geopolitical risk – resulting from the armed invasion of the Russian Federation into Ukraine – may imply an outflow of investments, PLN depreciation, liquidity

disruptions, a decline in asset prices and a decline in household activity. The ongoing conflict in the Middle East poses an additional threat.

- 3) Risk of questioning WIBOR – the risk concerns borrowers questioning loan agreements in which the WIBOR index is used.
- 4) Legal risks in the banking sector identified in relation to the uncertainty surrounding the interpretation of consumer protection legislation, in particular the increasing number of lawsuits related to the sanction of free credit.
- 5) Operational challenges related to the process of replacing the WIBOR index with a new reference index.

Cooperative banks

Cooperative banks offer a relatively simple range of bank services and products. As at 31 December 2024, there were 489 cooperative banks and 2 associating banks: Bank Polskiej Spółdzielczości SA and SGB-Bank SA. The cooperative banks and the associating banks formed two systems of institutional protection (BPS Association Protection System and SGB Cooperative Protection System), comprising 481 cooperative banks and both associating banks, while 8 cooperative banks operated outside the structures of associations and institutional protection systems. In 2024, due to merger processes, the number of cooperative banks decreased by 3 and 1 unassociated bank joined an institutional protection system and an association.

From September 2023 to September 2024, the assets of cooperative banks increased by 12.7%, i.e. by PLN 25.4 billion, to PLN 225.2 billion. The assets of the associating banks increased by 6.96%, i.e. by PLN 4.2 billion, to PLN 64.1 billion. The primary type of risk is credit risk – the share of loans in assets was approx. 57.7%. Cooperative banks are still primarily interested in financing business and agricultural activity (loans for this purpose account for approx. 66.6% of receivables from the non-financial sector). Such loan structure is undoubtedly affected by the history of cooperative banks – they were established primarily to finance the activity of farmers and craftsmen. Traditionally, cooperative banks collect deposits mainly from individuals. In cooperative banks, there is a growing surplus of deposits from the non-financial sector over loans to this sector. It is invested mainly in the associating banks and in debt instruments, mainly of the State Treasury and the NBP, and, to a lesser extent, in loans for local governments. Debt instruments of the State Treasury and the NBP accounted for 27.7% of the value of cooperative banks' assets.

From September 2023 to September 2024, the own funds of cooperative banks increased by 27.4%, to PLN 21.4 billion. The total capital ratio (TCR) of cooperative banks was 25.1%, compared to 22.6% in September 2023, while the Tier1 ratio was 24.7%, compared to 22.2% in September 2023. The increase in the TCR was significantly influenced by the profit distribution for 2023. In September 2024, all cooperative banks met the minimum requirement for own funds, taking the combined buffer requirement into account, except for one bank, which was acquired in October 2024 by another bank. As at the end of September 2024, the own funds of the associating banks were higher by 43.2% than in September 2023 and amounted to PLN 3.4 billion. Tier 1 capital accounted for 78.6% of own funds (71.6% in September 2023).

Cooperative banks have a fairly stable share in the banking market, amounting to approx. 6.9% of the total assets (together with the associating banks this share is approx. 8.9%). The share of deposits is approx. 10,6%.

Cooperative savings and credit unions (SKOK)

Pursuant to Article 3 of the *Act of 5 November 2009 on cooperative savings and credit unions* (consolidated text: Journal of Laws of 2024, item 512, as amended), the objective of cooperative savings and credit unions (hereinafter referred to as SKOK) is to collect cash only from its members, grant loans and credits to them, carry out financial settlements on their behalf, and provide insurance brokerage services.

Pursuant to Article 130(2)(1)(c) of the *AML/CFT Act*, read together with Article 63(1)1 of the above-mentioned *Act on cooperative savings and credit unions*, control over SKOKs is exercised by the National Cooperative Savings and Credit Union.

The financial services provided by SKOKs correspond, to the extent specified above, to those provided by banks. By accepting deposits, providing loans and credits, as well as offering financial settlements, SKOKs are thus an alternative to the banking sector system.

Along with banks, SKOKs are part of the financial sector that is of key importance for the state's economy. The financial sector, hence also SKOKs, due to the type of the services provided, is exposed to risks related to money laundering and financing of terrorism.

As at 31 December 2024, there were 18 SKOKs and the National Cooperative Savings and Credit Union (19 entities in total). In 2024, there were no mergers between SKOKs.

As at 30 September 2024, SKOKs showed a total net loss of PLN -11.39 million (at the end of December 2023, 18 SKOKs that were operating at that time showed a net loss of PLN -49.94 million).

Compared to the end of 2023, own funds of SKOKs decreased by 5.36%, i.e. by PLN 21.42 million, and amounted to PLN 399.40 million at the end of September 2024. The SKOKs' solvency ratio was 4.32%, lower than the 5% threshold required by law. Compared to the end of 2023, assets held by SKOKs decreased by 4.77%, i.e. by PLN 477.48 million to PLN 10,012.96 million.

The gross loan and credit portfolio decreased by 1.73%, i.e. by PLN 130.53 million, to PLN 7,542.43 million, while the value of deposits decreased by 4.76%, i.e. by PLN 446.32 million, to PLN 9,381.34 million.

The economic and financial situation of SKOKs varies. The operation of some of the SKOKs is stable, while the economic and financial situation of the others is difficult and requires remedial or restructuring measures. As at the end of September 2024, 9 SKOKs were required to implement a rehabilitation programme.

The SKOK sector is supervised by the KNF, whose activities are directed at mitigating the risks occurring in the individual entities of the sector in order to ensure the security of the deposits collected by these entities. The restructuring measures may involve, with the approval of the European Commission, public funds. In 2024, no such funds had to be mobilised.

Pursuant to Article 130(2)(1)(c) of the *AML/CFT Act*, the National Cooperative Savings and Credit Union exercises control over SKOKs. The National Cooperative Savings and Credit

Union has dedicated neither human nor financial resources solely for the implementation of control tasks in the field of counteracting money laundering and financing of terrorism (all employees and units participating in this process also perform other tasks entrusted to them, including other types of controls).

Payment institutions sector

The Polish Financial Supervision Authority (KNF) supervises, among others, domestic payment institutions (DPI), domestic electronic money institutions (DEMI), small payment institutions (SPI), payment service providers (PSP) and providers offering exclusively the account information service (AISP). These entities are authorised to render payment services, but there are significant differences between them – e.g. in terms of the range of authorised payment services, the territorial scope of activities, the legal form, the requirements necessary to obtain the right to conduct such activities (licensing requirements), or in terms of capital requirements.

The supervisory activities undertaken by the KNF with regard to DPIs include, in particular, the verification of standard statutory reporting, the analysis of the financial results achieved in the context of their compliance with the financial plans and statutory requirements submitted at the licensing procedure stage, as well as the examination of DPI's compliance with applicable national and Community regulations.

As at 31 December 2024, the Register of Electronic Money Providers and Issuers included: 46 DPIs, 184 SPIs, 15 AISPs, 1 DEMIs and 965 PSPs.⁶ As at the end of Q3 2024, DPI's own funds amounted to PLN 1.9 billion. According to the reporting information submitted by DPIs to the KNF, between 1 January 2024 and 30 September 2024, DPIs performed a total of 4.16 billion payment transactions with a total value of PLN 482.96 billion. In the same period, SPIs performed a total of 25.19 million transactions worth PLN 5.23 billion. For comparison, in the same period, Krajowa Izba Rozliczeniowa S.A. (Polish National Clearing House) processed 1.67 billion payment orders worth PLN 6.72 trillion in the Elixir System; it should be noted, however, that some of the transactions made by the DPIs are cleared in other clearing systems, e.g. Express Elixir, Euro Elixir and BlueCash. Therefore, the importance of the DPI sector in the macroeconomic context is negligible.

Life insurance sector

As at the end of Q3 2024, insurance class I (life insurance) was composed of 23 insurance companies authorised to carry out insurance activity (all of them carried out operating activities). Of these, 3 life insurance companies were in the process of merging, which took place at the beginning of Q4 2024.

Life insurance companies operated approx. 11.82 million insurance agreements. In the revenue structure of insurance companies, gross premium written prevailed. During the three quarters of 2024, its amount in the life insurance class was PLN 17.70 billion and accounted for 27.99% of the total gross premium written of the entire insurance sector.

As at the end of Q3 2024, the structure of direct insurance in class I was dominated by life insurance (group 1), accounting for 44.12% of the gross premium written. The second position

⁶ Applies to payment service providers.

was occupied by supplemental accident and sickness insurance (group 5), accounting for 38.06% of the gross premium written. This was 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 16.78% of the total premium of the class.

In the three quarters of 2024, life insurance companies paid out gross claims and benefits in the amount of PLN 12.16 billion. As at the end of Q3 2024, life insurance companies also established gross technical and insurance provisions in the amount of PLN 73.92 billion.

The net profit of class I insurance companies was PLN 3.05 billion, while income tax reported by these insurance companies amounted to PLN 0.62 billion.

As at the end of Q3 2024, the total amount of assets of life insurance companies was PLN 91.10 billion, of which:

- PLN 33.15 billion were funds supporting the economy and public finance through domestic bonds and other fixed income securities;
- PLN 6.17 billion were funds invested in company shares and other variable-yield securities.

As at the end of Q3 2024, life insurance companies reported equity of PLN 11.31 billion, which accounted for 12.41% of their assets.

As at the end of Q3 2024, the solvency of life insurance companies was at a high, secure level. All class I insurance companies showed coverage of the solvency ratios (understood as the minimum from the amount of eligible own funds to the capital solvency requirement and eligible basic own funds to the minimum capital requirement), including 20 class I insurance companies with solvency ratios above 175%. For class I, the following factors had the greatest impact on the extent of the capital solvency requirement: customer churn risk, mortality risk, catastrophe risk in life insurance, and the risk of expenses in life insurance (as part of actuarial risk in life insurance) as well as interest rate risk, asset concentration risk, stock price risk and credit spread risk (within the market risk).

Capital sector

Brokerage houses and offices

The primary legal act regulating the operation of brokerage houses and offices in the territory of Poland is the *Act of 29 July 2005 on trading in financial instruments* (consolidated text: Journal of Laws of 2024, item 772, as amended).

Brokerage activities involve, among others, accepting and transferring orders for buying or selling financial instruments, proprietary buying or selling securities, managing portfolios consisting of one or more financial instruments, investment advisory, offering financial instruments, and rendering services under agreements on investment and services sub-underwriting. Brokerage activities may be carried by an investment firm being a brokerage house or a bank carrying out brokerage activities. Brokerage houses may carry out brokerage activities in the form of a joint stock company, a limited joint-stock partnership, a limited-liability company, a limited partnership, a partnership or a general partnership. An entity that intends to carry out brokerage activities must obtain an authorisation of the KNF.

As at the end of 2024, authorisations to carry out brokerage activities were held by:

- 27 brokerage houses and 9 banks in different respects provided for in Article 69(2) and (4) of the *Act of 29 July 2005 on trading in financial instruments*;
- 12 custodian banks.

In 2024, the authorisation to carry out brokerage activities was found to have expired for 1 commodity brokerage house – i.e. activities under Article 38(2) of the *Act of 26 October 2000 on commodity exchanges* (consolidated text: Journal of Laws of 2024, item 910, as amended).

Among the entities identified above, 1 brokerage house has not commenced activities covered by the licences held in 2024.

Table 1. Numbers of entities, by category, carrying out brokerage activities in 2019 – 2024

Type of entity	2019	2020	2021	2022	2023	2024
Brokerage houses	37	36	36	33	30	27
Commodity brokerage houses	1	1	1	1	1	1
Banks conducting brokerage activities	9	9	9	9	9	9
Custodian banks	12	11	11	9	12	12
TOTAL	59	57	57	52	52	49

As part of brokerage activities, investment companies carry out activities involving, in particular:

- accepting and transferring orders for buying or selling financial instruments;
- implementing orders referred to above on the account of the ordering party;
- proprietary buying or selling securities;
- managing portfolios consisting of one or more financial instruments;
- investment advisory;
- offering financial instruments;
- providing services as part of the performance of concluded underwriting contracts, or concluding and performing other agreements of a similar nature, as long as they relate to financial instruments.

Investment companies differ in terms of the scope of their brokerage licences. There are companies that perform one type of brokerage activity as well as companies that offer a wide range of brokerage services.

Brokerage houses

As at 31 December 2024, out of the 30 brokerage houses authorised to conduct brokerage activities, 15 held financial instruments or cash of customers. These entities, as a rule, also perform a much wider range of activities, and therefore have greater opportunities to diversify the sources of revenue generation.

As at 31 December 2024, brokerage houses kept 1,639,583 financial instrument accounts of their customers (an increase of 46.18% compared to 31 December 2023), with a total value of financial instruments of PLN 148,891,743,609 (a decrease of 3.16% compared to

31 December 2023). The amount of customers' cash deposited on cash accounts was PLN 8,230,491,889 (an increase of 6.05% compared to 31 December 2023).

As at the end of 2024, 8 brokerage houses provided services involving the management of customers' assets. As at 31 December 2024, these entities managed customers' assets worth PLN 8,517,955,175 (an increase of 21.90% compared to 31 December 2023).

According to the data contained in their December monthly reports, in 2025, the brokerage houses generated a net profit of PLN 1,017,072,034 (representing 104.63% of the 2023 net profit). As at 31 December 2024, the equity of the brokerage houses amounted to PLN 2,866,998,413 (representing 109.88% of equity as at 31 December 2023) and their total assets amounted to PLN 12,857,063,544 (representing 104.90% of total assets as at 31 December 2023). Monthly reports contain preliminary data that is not subject to verification by an auditor.

Commodity brokerage houses

In October 2024, the Extraordinary Meeting of Shareholders of the only commodity brokerage house licensed by the KNF passed a resolution to dissolve the company after liquidation.

Brokerage offices

As at 31 December 2024, brokerage offices kept for their customers 2,022,469 financial instrument accounts (an increase of 7.63% compared to 31 December 2023), with a total value of financial instruments of PLN 530,405,956,644 (an increase of 4.52% compared to 31 December 2023). The amount of customers' cash deposited in cash accounts used to handle financial instrument accounts was PLN 9,930,820,439 (an increase of 7.96% compared to 31 December 2023). By managing portfolios consisting of one or more financial instruments, brokerage offices managed customers' assets in the amount of PLN 2,427,743,409 (an increase of 2.20% compared to 31 December 2023).

Custodian banks

As at 31 December 2024, custodian banks operated 39,239 securities accounts (a decrease of 0.47% compared to 31 December 2023) with assets in the amount of PLN 1,001,528,665,650 (an increase 7.01% compared to 31 December 2023).

Investment fund management companies (TFI)

The rules for establishing and operating investment fund management companies registered in the territory of the Republic of Poland are defined in the *Act of 27 May 2004 on investment funds and the management of alternative investment funds* (consolidated text: Journal of Laws of 2024, item 1034, as amended).

An investment fund is a legal person whose sole activity consists in investing cash collected through public, and in the cases specified in the aforementioned Act – also non-public, offering of the purchase of investment units or investment certificates in securities, money market instruments, and other property rights specified in this Act. An investment fund is managed by an investment fund management company.

As at 31 December 2024, there were 55 investment fund management companies authorised by the KNF, that managed assets in the total amount of PLN 501.7 billion. As at the end of 2014,

the investment fund management companies managed 605 investment funds, including those in liquidation. The total number of investment funds included 46 open-ended investment funds, 63 specialist open-ended investment funds, and 496 closed-ended investment funds. As at 31 December 2024, the total value of the investment funds' assets was PLN 429.9 billion. The value of the portfolios consisting of one or more financial instruments managed by investment fund management companies was PLN 69.9 billion.

The value of assets deposited with the investment funds as at the end of 2024 accounted for approx. 13% of GDP for 2023 and for approx. 29% of the capitalisation of the Stock Exchange as at the end of December 2024. It should also be noted that the total assets of the investment funds as at the end of 2024 were 102% higher than the value of the assets of open-ended pension funds.

As at 31 December 2024, the total assets of the investment fund management companies was PLN 3,521,995 thousand, 46% of which was cash in the amount of PLN 1,625,718 thousand. The total value of the equity of the investment fund management companies as at the end of 2024 was PLN 2,625,867 thousand. In the period from 1 January 2024 to 31 December 2024, the total net profit of the investment fund management companies was PLN 1,004,287 thousand. In 2024, the investment fund management companies generated total revenue of PLN 4,368,392 thousand, which included mainly revenue from investment fund management of PLN 3,995,824 thousand. The total costs incurred by the investment fund management companies in 2024 amounted to PLN 3,134,505 thousand, 18% of which were variable distribution costs of PLN 594,843 thousand.

Currency exchange office operators⁷

Performing the tasks specified in the *Act of 27 July 2002 – Foreign Exchange Law* (consolidated text: Journal of Laws of 2024, item 309) and in the *AML/CFT Act*, the President of the NBP keeps a register of currency exchange services and exercises control over currency exchange services, as well as supervises the fulfilment by currency exchange office operators of their obligations relating to counteracting money laundering and terrorism financing.

As at 31 December 2024, the register included 2,212 currency exchange office operators and 4,652 currency exchange offices. As at 31 December 2024, currency exchange services were provided in 4,446 currency exchange offices, while in 206 ones the provision of these services was suspended.

Table 2. Value of foreign currencies bought and sold in currency exchange offices in Q4 2023 and in Q1, Q2 and Q3 2024 (in PLN million)

Period	Foreign currencies bought	Foreign currencies sold	Balance of turnover
Q4 2023	19,466	15,039	4,427
Q1 2024	17,127	13,462	3,665
Q2 2024	19,931	15,043	4,888
Q3 2024	20,731	16,043	4,688

⁷ Besides currency exchange office operators, banks and branches of credit institutions, currency exchange is conducted also by other entities that do it via the Internet. There are also entities providing services consisting in collecting and matching currency exchange orders from various customers and organising/enabling such exchange between them. Pursuant to Article 2(1)(11) of the *AML/CFT Act*, they are obligated institutions.

In 2024, controls were carried out at 368 currency exchange office operators. The controls covered 602 currency exchange offices.

Other institutions

Besides the above-mentioned obligated institutions, there are also other obligated institutions operating in the financial market, i.e. lending institutions referred to in Article 2(1)(25) of the *AML/CFT Act*, as well as some financial institutions.

The provisions of Chapter 5a of the *Act of 12 May 2011 on consumer loan* (consolidated text: Journal of Laws of 2024, item 1497, as amended) set out conditions that must be met by a lending institutions to be permitted to operate. In accordance with Article 59aa(1) of the above-mentioned Act, the lending institution may commence business activity following its entry into the register of lending institutions. The register of lending institutions has been kept by the KNF since 2017. According to information available on the website, the register listed 540 lending institutions⁸ compared to 527 ones in 2023.

As for the definition of a financial institution, the *AML/CFT Act* refers to the provisions of the *Act of 29 August 1997 – Banking Law* (consolidated text: Journal of Laws of 2024, item 1646, as amended) that defines it in Article 4(1)(7) as “the financial institution referred to in Article 4(1)(26) of *Regulation No 575/2013*”. The invoked provision of *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 and amending Regulation (EU) No 648/2012* (OJ EU L 176 27.6.2013, p. 1) stipulates that “«financial institution» means an undertaking other than an institution⁹, 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*, including 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*, and asset management companies, but excluding insurance holding companies and mixed-activity insurance holding companies”. Thus, factoring and leasing companies (with respect to financial leasing) and entities whose primary activity involves “consulting services for economic enterprises concerning their capital structure, industrial strategy and the related issues, as well as consulting and services related to mergers and acquisitions of economic enterprises”¹⁰ should be considered financial institutions that are not other obligated institutions specified in the *AML/CFT Act*.

According to the Statistics Poland information¹¹ of 7 February 2025 on national economy entities entered in the National Official Business Register REGON, as at the end of 2024, the register listed 601 (compared to 619 in 2023) economic entities reporting economic activity involving financial leasing – Polish Classification of Activities (PKD) 64.91.Z. According to

⁸ <https://rkip.knf.gov.pl/index.html?type=RIP>, read on 7.02.2025.

⁹ Defined in Article 4(1)(3) of *Regulation 575/2013* as “a credit institution or an investment firm”.

¹⁰ Point 9 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* (OJ EU L No. 176 of 27.06.2013, p. 338).

¹¹ <https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2024.7.14.html>, access on 7.02.2025.

the above-mentioned Statistics Poland data, most companies in this industry were registered in the Mazowieckie Voivodeship – 217 (compared to 222 in 2023).

Financial (capital, investment) leasing consists in the transfer by the financing party (lessor) of the right to use certain fixed assets (or the right to use and obtain benefits) to the user (lessee) for a definite period in exchange for appropriate fees (leasing instalments). The ownership of the fixed asset may, but does not have to, be ultimately transferred to the leaseholder. This type of lease covers all or virtually all costs, including interest.

According to the Statistics Poland data¹² contained in quarterly information on national economy entities as at 31 December 2024, the National Official Business Register REGON included (without natural persons running only private farms) a total of 8,194 (compared to 8,251 in 2023) entities reporting the activity defined by the Polish Classification of Activities (PKD) code – 64.99.Z, i.e. other financial service activities, except insurance and pension funding not elsewhere classified (this subclass includes, among others, factoring services).

Apart from the above-mentioned financial institutions, Krajowy Depozyt Papierów Wartościowych S.A. (Central Securities Depository of Poland), hereinafter referred to as 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.

KDPW S.A. and KDPW_CCP, along with GPW S.A. and BondSpot S.A., are classified by the KNF as entities of the capital market infrastructure. KDPW S.A. is a central depository for securities and it is tasked, among others, with operating and supervising the securities registration system and the settlement system for transactions in financial instruments, as well as with supervising the compliance of the issue limit value with the number of securities on the market, handling corporate events, performing issuers' obligations, and operating a mandatory compensation system. KDPW_CCP S.A. is a clearing house, owned by the KDPW in 100%.

2.2.2. OTHER CATEGORIES OF OBLIGATED INSTITUTIONS

Obligated institutions pursuing legal professions

Legal professions are professions of public trust that are pursued in the scope and manner described in specific provisions. They are usually regulated, i.e. they are subject to control by both the state and particular corporations. The pursuit of a liberal legal profession requires high skills and knowledge.

Pursuant to Article 1(1)-(2) of the *Act of 14 February 1991 on Notary* (consolidated text: Journal of Laws of 2024, item 1001, as amended), a notary acts within the scope of his/her powers as a person of public trust, taking advantage of the protection conferred on public officers, whereas notarial activities performed by the notary in accordance with law, take the form of an official document. The notary's tasks are to ensure the security and regularity of legal transactions (in accordance with Article 80(2) of the above-mentioned *Act*, in the course

¹² <https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2024.7.14.html>, access on 7.02.2025.

of their activities, the notary is obliged to ensure due protection of the rights and legitimate interests of the parties and other individuals for whom this activity may cause legal effects).

According to information provided by the National Council of Notaries, as at 14 February 2025, the profession of notary was practised by 4,045 individuals (compared to 3,954 in 2022)¹³.

Pursuant to Article 2(1)(13) and (13a) of the *AML/CFT Act*, notaries are obligated institutions in so far as they perform their activities in the form of a notarial deed, including:

- transfer of the ownership of an asset, including the sale, exchange or donation of a 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 premises¹⁴;
- in-kind contribution following a company establishment;
- 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;
- transformation or merger of companies;
- transfer of an enterprise;
- transfer of shares in a company;
- keeping a register of shareholders of simple joint-stock companies and taking action related thereto.

An attorney is a lawyer providing legal assistance in accordance with the *Act of 26 May 1982 – Law of the Bar* (consolidated text: Journal of Laws of 2024, item 1564, as amended). An attorney is obliged to keep confidential any facts they may become aware of in the course of providing legal assistance. The obligation of professional secrecy does not apply to information made available under the AML/CFT regulations – to the extent specified in these regulations.

According to information included in the National Register of Attorneys and Attorney Trainees kept by the Polish Bar Association, as at 14 February 2025, there were 22,893 attorneys (compared to 22,232 as at 12 March 2024) practicing their profession¹⁵, and 108 (compared to 101 as at 12 March 2024) foreign lawyers providing legal assistance.¹⁶

As for a legal counsel, this is a lawyer providing legal assistance in accordance with the *Act of 6 July 1982 on legal advisers* (consolidated text: Journal of Laws of 2024, item 499, as amended). In particular, legal advisers provide legal advice and consultation, prepare legal opinions and draft legal acts, as well as act as representatives or defenders before authorities

¹³ <https://krm.org.pl> – information on the website from tab [Europejski Spis Notariuszy – wyszukiwarka](#), access on 14.02.2025.

¹⁴ Alleged promise is a state of waiting for the establishment of separate ownership of premises. Its duration occurs between the signing of the agreement for the construction of the premises and lasts until the separation of the flat and the entry in the land and mortgage register.

¹⁵ <https://rejestradvokatow.pl>, access on 14.02.2025

¹⁶ <http://rejestradvokatow.pl/>, access on 14.02.2025

and courts (including the Supreme Court, the Constitutional Court, the Supreme Administrative Court, the Court of Justice of the European Union and the European Court of Human Rights).

According to the information contained in the search engine of legal advisers, provided by the National Chamber of Legal Advisers, as at 14 February 2025, there were 54,810 legal advisers¹⁷ (compared to 53,360 ones as at 12 March 2024).

Like legal advisers and foreign lawyers¹⁸, attorneys are obligated institutions in so far as they provide customers with legal assistance or tax advisory in the area of:

- purchase or sale of real estate, an enterprise or an organised part of an enterprise;
- management of cash, financial instruments or other customer's assets;
- concluding an agreement for operating a bank account, a securities account or performing activities related to keeping these accounts;
- in-kind contribution to a capital company or increasing the share capital of a capital company;
- establishing, operating or managing capital companies or trusts.

According to the information on the website of the Revenue Administration Regional Office in Katowice, as at 24 February 2025, there were 2,183 entities listed in the register of activities for companies and trusts.

Tax advisors and statutory auditors

Tax advisors practice their profession in accordance with the *Act of 5 July 1996 on tax advisory services* (consolidated text: Journal of Laws of 2021, item 2117). In accordance with Article 2(1) of the aforementioned *Act*, tax advisory services include:

- providing taxpayers, tax remitters and collectors, at their request or on their behalf, with advice, opinions and explanations concerning their tax and customs obligations as well as the administrative enforcement procedure in relation to these obligations;
- keeping, on behalf of and for the benefit of taxpayers, tax remitters and collectors, accounting records, tax books and other records for tax purposes, and providing them with respective assistance;
- drafting, on behalf of and for the benefit of taxpayers, tax remitters and collectors, tax returns and declarations, or providing them with respective assistance;
- representing taxpayers, tax remitters and collectors in proceedings before public administration bodies and with respect to judicial review of decisions, rulings and other administrative acts in cases referred to in the first subparagraph.

The activities referred to in the first and last subparagraphs may be carried out only by the entities indicated in the aforementioned *Act*, i.e. natural persons entered in the list of tax

¹⁷ [Rejestradow.pl](https://rejestradow.pl), access on 14.02.2025.

¹⁸ Excluding legal advisers and foreign lawyers practicing their profession under an employment relationship or service in offices providing services to public administration authorities, other government or local government organisational units, and in entities other than companies referred to in Article 8(1) of the *Act of 6 July 1982 on Legal Advisers*.

advisors, attorneys and legal advisers, and in the case of the activities referred to in the first subparagraph – also statutory auditors. The following entities are also entitled to professionally perform the activities mentioned in the first and fourth subparagraphs (provided that these activities are performed only by persons employed in these entities, indicated in the preceding sentence):

- professional organisations with legal personality, cooperatives, associations or chambers of commerce, as long as their statutory activities include also tax advisory services provided exclusively to their members;
- audit firms authorised under other provisions to audit financial statements;
- limited-liability companies or joint stock companies that meet the conditions listed in Article 4(1)(3) of the aforementioned *Act*.

Professional tax advisory services are subject to statutory protection and they must not be carried out by unauthorised entities that are otherwise subject to a fine. The tax advisor is obliged to conclude a civil-liability insurance agreement for the tax services they provide.

Tax advisors providing legal assistance or tax advisory services to clients are obligated institutions to the same extent as attorneys, legal advisers or foreign lawyers. Moreover, they are obligated institutions in so far as they provide tax advisory services other than those listed in Article 2(1)(14) of the *AML/CFT Act*.

As at 18 February 2025, there were 9,049 registered tax advisors¹⁹ (compared to 8,942 ones in 2023).

Statutory auditors practise their profession in accordance with the *Act of 11 May 2017 on statutory auditors, audit firms and public supervision* (Journal of Laws of 2024, item 1035, as amended). Pursuant to Article 3(1) of the aforementioned Act, in the framework of their professional activity, statutory auditors conduct financial audits and provide attestation services other than financial audits, that are not reserved to be performed by statutory auditors, as well as related services. The statutory auditor may practice their profession as: a natural person conducting business activity in their own name and on their own behalf or as a partner of an audit firm, or as a natural person under an employment relationship with an audit firm, or as a natural person (including a person conducting business activity otherwise than specified above) who has concluded a civil-law contract with an audit firm.

According to information from the register of statutory auditors, maintained by the National Chamber of Statutory Auditors – as at 18 February 2025, – there were 4,829 statutory auditors²⁰ (compared to 4,919 as at 13 March 2024) and 1,187 audit firms²¹ (compared to 1,229 as at 13 March 2024).

Entities carrying out business activities involving games of chance, betting, card games and games on gaming machines

The operation of the gambling market is regulated by the *Act of 19 November 2009 – Gambling Law* (consolidated text: Journal of Laws of 2023, item 227, as amended) and the implementing

¹⁹ <https://kidp.pl>, access on 18.02.2025

²⁰ Register of statutory auditors | PIBR, accessed on 18.02.2025.

²¹ <https://strefa.pana.gov.pl/wyszukiwarka/>, access on 18.02.2025

regulations to this *Act*. According to them, gambling games are games of chance, betting, card games and games 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, raffles, 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 – these are sweepstakes. Besides sweepstakes, betting includes also bookmaking, i.e. 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.

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.

Carrying out business activity involving draw-based games, cash lotteries, telebingo games and games on gaming machines outside casinos, and arranging online gambling (except for betting and promotional lotteries) is subject to the state monopoly. The state monopoly is exercised by the minister competent for state assets, who establishes for this purpose, in consultation with the minister competent for public finance, single-person companies of the State Treasury.

The above-mentioned *Act of 19 November 2009 – Gambling Law* provides that the organisation of gambling requires – depending on the type of the game – a licence or authorisation of the minister competent for public finance or an authorisation of the competent director of the Revenue Administration Regional Office (IAS).

As at 18 February 2025, there were 51 licences issued for operating casinos, specifying the location of each of the casinos²². As at the same date, there were a total of 21 entities operating in the betting market²³, authorised by the Minister of Finance to organise betting. An authorisation issued by the Minister of Finance for organising betting in betting shops was held by 7 entities, while 18 entities held this Minister's authorisation for organising and operating betting online. One entity was authorised to organise and conduct other types of gambling online, including games on gaming machines, card games, cylindrical games, dice games (www.totalcasino.pl) as well as draw-based games and cash lotteries (www.lotto.pl).

Postal operator

Pursuant to Article 3(12) of the *Act of 23 November 2012 – Postal Law* (consolidated text: Journal of Laws of 2023, item 1640), a postal operator is an economic operator authorised to perform postal activity based on 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

²² <https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/kasyna-gry/>, access on 18.02.2025

²³ [Zakłady wzajemne i gry hazardowe przez Internet \(podatki.gov.pl\)](https://www.podatki.gov.pl/zaklady-wzajemne-i-gry-hazardowe-przez-internet/), access on 18.02.2025

obliged to provide postal services. In accordance with the decision of the President of the Office of Electronic Communications, from 1 January 2016 to 31 December 2025, Poczta Polska S.A. is the operator designated to provide universal postal services in the Republic of Poland.

According to the information contained in the register of postal operators kept by the President of the Office of Electronic Communications, as at 20 February 2025, there were 259 postal operators²⁴ (compared to 279 as at 13 March 2024).

Foundations and associations

A foundation is a legal form of a non-governmental organisation in which capital allocated for a specific purpose plays an important role. Pursuant to Article 1 of the *Act of 6 April 1984 on foundations* (consolidated text: Journal of Laws of 2023, item 166) “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”. Foundations may pursue several objectives at the same time.

According to Statistics Poland information of 20 December 2024, there were 20.3 thousand foundations in Poland (data as at 31 December 2023).²⁵

Foundations 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.

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”.

An association independently determines its objectives, action programmes and organisational structures and adopts internal acts concerning its activities, while its operations are based on the voluntary work of its members. An association may employ staff, including its members, to perform its activities.

According to Statistics Poland information of 20 December 2024, there were 68.9 thousand associations (data as at 31 December 2023).²⁶

Only those 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.

²⁴ <https://bip.uke.gov.pl/rop/rejestr-operatorow-pocztowych>, access on 20.02.2025

²⁵ <https://stat.gov.pl/obszary-tematyczne/gospodarka-spoleczna-wolontariat/gospodarka-spoleczna-trzeci-sektor/podmioty-ekonomii-spolecznej-w-2023-r-,23,2.html>, access on 20.02.2025

²⁶ <https://stat.gov.pl/obszary-tematyczne/gospodarka-spoleczna-wolontariat/gospodarka-spoleczna-trzeci-sektor/podmioty-ekonomii-spolecznej-w-2023-r-,23,2.html>, access on 20.02.2025

According to information obtained in accordance with Article 14(4) of the *AML/CFT Act* from governors of districts, governors of provinces (voivodes) and ministers²⁷, a total of 14 obligated institutions were identified (as at 31 December 2024)²⁸. Among the obligated institutions supervised by the aforementioned authorities, there were 4 associations, while in 10 cases the competent authorities defined the legal form of the supervised entity as a foundation. Based on the information provided to the GIFI, 98% of governors of districts 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 2% of them assessed their human and financial resources as insufficient. In the vast majority of governor's of districts offices, tasks related to the implementation of AML/CFT obligations were carried out by one to three employees.

Other non-financial obligated institutions

A substantial group of obligated institutions operating outside the financial market comprises economic operators conducting non-regulated activity, mainly under the provisions of the *Act of 6 March 2018 – Entrepreneurs' Law* (consolidated text: Journal of Laws of 2024, item 236, as amended), hereinafter referred to as *Entrepreneurs' Law*. These include obligated institutions specified in Article 2(1) (10a), (12), (15a), (16)-(18), (23)-(24), (24a) and 26²⁹ of the *AML/CFT Act*.

Obligated institutions referred to in Article 2(1)(12) of the *AML/CFT Act* include entities conducting business activities consisting in the provision of services in the field of: exchange between virtual currencies and legal tender, exchange between virtual currencies, brokerage in the exchange referred to in point (a) or (b), operating accounts referred to in Article 2(17)(e) of the *AML/CFT Act*, i.e. ones maintained in the form of electronic identification data sets enabling authorised persons to use virtual currency units, among others to conduct their exchange transactions.

²⁷ As part of their supervision or control, the performance by obligated institutions of their AML/CFT obligations is controlled by governors of provinces (voivodes) or governors of districts – in relation to associations, and ministers or governors of districts – in relation to foundations, in accordance with the rules set out in this Act.

²⁸ The information provided by ministers, governors of districts and governors of provinces (voivodes) was based on their knowledge. Some respondents – particularly governors of districts – pointed out to the limited ability to determine which associations met the conditions specified in Article 2(1)(22) of the *AML/CFT Act* (i.e. during inspections carried out in accordance with other provisions or by collecting declarations from the associations).

²⁹ Economic operators conducting pawnbroking activities referred to in the *Act of 14 April 2023 on consumer pawnbroking loans* (Journal of Laws of 2024, item 1111). Article 2(1)(26) was added by the *Act of 14 April 2023* (Journal of Laws of 2024, item 1111), that entered into force on 7 January 2024. Economic operators conducting pawnbroking activities are obliged to obtain an entry in the register. The register of economic operators conducting pawnbroking activities is kept by the KNF. Conducting pawnbroking activities without an entry in the register is a prohibited act punishable by a fine of up to PLN 500,000. The *Act on pawnbroking activities* does not provide for the supervision of the KNF over economic operators conducting pawnbroking activities. This means, in particular, that the KNF is not authorised to request information and explanations from these entities and to control their activities for their compliance with law, or to assess whether they meet the requirements provided for by law. Compliance with the *Act on pawnbroking activities* is controlled by the Trade Inspection.

On 30 December 2024, the *MiCA Regulation*³⁰ became fully applicable.³¹ The Regulation lays down uniform requirements for the offer to the public and admission to trading on a trading platform of crypto-assets other than asset-referenced tokens and e-money tokens, as well as requirements for crypto-asset service providers.

A draft Act on crypto-assets is currently being developed; it envisages the introduction of new solutions in the area of the crypto-asset market sector, aiming to fulfil the tasks arising from the MiCA Regulation.³²

In accordance with the information available on the website of the Regional Revenue Administration Office in Katowice³³, as at 20 February 2025, the register of virtual currency service providers included 1841 entities.

The number of bitcoin ATMs in Poland (but also worldwide) is constantly growing. The growth rate of 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 amounts of commission on such transactions). In one bitcoin ATM, it is also possible to buy/sell particular types of cryptocurrencies.

Cryptocurrency exchange offices provide their services 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.

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.

According to information from the website <https://coinatmradar.com/bitcoin-atm-near-me/>, as of 24 February 2025, there are at least 291 bitcoin ATMS operating in Poland³⁴ (compared to 249 such devices in 2023).

Another group of obligated institutions are entities conducting real estate trading activities. A broker³⁵ – an economic operator conducting business activities involving real estate intermediation – may participate in such activities. Real estate intermediation consist in the paid performance of activities aimed at concluding contracts by other persons. The scope of real estate brokerage services is specified by a real estate intermediation contract. The contract must be executed in writing or in electronic form under pain of nullity. It is not possible to specify the actual number of real estate intermediaries as each economic operator may perform real

³⁰ Regulation (EU) No 2023/1114 - Market in Crypto Assets Regulation (MiCA).

³¹ The MiCA Regulation entered into force on 29 June 2023.

³² Draft Act on the crypto-asset market, UC2 list number, available at:

<https://legislacja.rcl.gov.pl/projekt/12382311/katalog/13040387#13040387> read date: 12.12.2024

³³ <https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych>, access on 20.02.2025

³⁴ <https://coinatmradar.com/bitcoin-atm-near-me/>, access on 24.02.2025

³⁵ Pursuant to Article 2(1)(18) of the *AML/CFT Act*, real estate brokers within the meaning of the *Act on real estate management* are obligated institutions, except for real estate intermediation aimed at concluding a rental or lease agreement for real estate or a part thereof, where the monthly rent is less than the equivalent of EUR 10,000.

estate intermediation, provided that they hold civil liability insurance for damage caused in connection with the performance of these activities.

According to the Statistics Poland data contained in the quarterly information on national economy entities, as at 31 December 2024, the National Official Business Register REGON (excluding natural persons running solely private farms) included a total of 23,876 entities (compared to 22,671 in 2023) reporting the activity defined by the Polish Classification of Activities (PKD) code 6831Z, i.e. real estate brokerage³⁶.

In accordance with Article 76a(1) of the *Accounting Act of 29 September 1994* (Journal of Laws of 2023, item 120, as amended), bookkeeping services are a business activity within the meaning of the provisions of the aforementioned *Entrepreneurs' Law*, consisting in the provision of services in the area of:

- keeping accounting records based on accounting evidence, in which economic events are recorded in the chronological and continuous order;
- determining or verifying on a regular basis, by means of stocktaking, the actual balance of assets and liabilities;
- measurement of assets and liabilities and determining financial profit/(loss);
- drawing up financial statements;
- collecting and storing accounting evidence and other documents provided for in the aforementioned *Act*.

Bookkeeping services may be rendered by any economic operator, provided that bookkeeping activities are performed by persons who have full legal capacity and have not been convicted by a final court judgement of an offence against the reliability of documents, property, economic transactions, trading in money and securities, of a fiscal offence and of any offences specified in Chapter 9 of the aforementioned *Act*. An economic operator conducting such activity is also required to conclude, no later than on the day preceding the first day of performing its business activity, a civil-liability insurance agreement for damage caused in connection with its economic activity in the field of bookkeeping services.

Pursuant to Article 2(1)(16) of the *AML/CFT Act*, obligated institutions also include economic operators within the meaning of the *Entrepreneurs' Law*, that are not other obligated institutions, providing services in the area of:

- establishing a legal person or an organisational unit without legal personality;
- serving as a member of the management board or enabling 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, address of establishment or address for correspondence and other related services to a legal person or an organisational unit without legal personality;

³⁶<https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2024,7,14.html>, access on 24.02.2025

- acting or enabling another person to act as the trustee of a trust established by means of a legal act;
- acting or enabling another person to act as a person exercising rights attached to stocks or shares to the benefit of an entity other than a company listed on the regulated market subject to the requirements related to information disclosure in compliance with the European Union law or subject to equivalent international standards.

Moreover, pursuant to Article 2(1)(15a) of the *AML/CFT Act*, obligated institutions also include economic operators within the meaning of the *Entrepreneurs' Law*, whose primary business activities include the provision of services consisting in preparing tax returns, keeping tax books, providing advice, opinions or explanations regarding tax or customs legal provisions, that are not other obligated institutions.

According to the Statistics Poland data contained in the quarterly information on national economy entities as at 31 December 2024, the National Official Business Register REGON included (excluding natural persons running only private farms) a total of 28,957 entities (compared to 26,156 in 2022) reporting the activity defined by the Polish Classification of Activities (PKD) code – 82.11.Z, i.e. office administration services³⁷. This sub-class covers “activities related to the day-to-day office administration, such as reception services, financial planning, accounting, bookkeeping, HR services and mail delivery, performed on commission”.

One of the banking activities specified in Article 5 of the *Act of 29 August 1997 – Banking Law* consists in providing access to a safe deposit box, provided that such activities are performed by banks. However, providing access to safe deposit boxes may also be economic activity within the meaning of the *Entrepreneurs' Law*.

According to data as at 12 March 2025, 30 entities were engaged in the activity of renting safe deposit boxes³⁸, of which:

- 24 entities were cooperative banks,
- 3 entities were commercial banks,
- 3 entities were entrepreneurs in the safety deposit box business.

A relatively large category of obligated institutions comprising business in various sectors is composed of economic operators that accept or make cash payments for commodities in the amount equal to or exceeding the equivalent of EUR 10,000, regardless of whether the payment is made as a single transaction or as a series of transactions which seem to be related to each other. Although Article 19 of the *Entrepreneurs' Law* obliges economic operators to make and accept payments related to their business activities through their payment accounts, whenever the one-off value of a transaction, regardless of the number of resulting payments, exceeds PLN 15,000 or its equivalent, it applies only to business-to-business transactions.

³⁷ <https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2024.7.14.html>, access on 24.02.2025

³⁸ Data on entities providing access to safe deposit boxes is taken from the SINF system (as at 12 March 2025).

Pursuant to Article 2(1)(24a) of the *AML/CFT Act*, obligated institutions also include economic operators within the meaning of the *Entrepreneurs' 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* (Journal of Laws of 2022, item 361, as amended), 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, 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*, 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.

The indicated new category of obligated institutions is to reduce the shadow economy in the area of alternative investments that have been developing dynamically recently. The group of obligated institutions that apply customer due diligence measures under the *AML/CFT Act* includes in this aspect, among others, organisations trading in works of art or acting as brokers therein (also if such trade is carried out through art galleries and auction houses), where the value of the transaction or series of related transactions is at least EUR 10,000.

Brokers in trade in works of art or persons storing such goods are also obliged to perform similar activities. This concerns mainly art dealers, small galleries, and economic operators offering the storage of works of art and collectibles. This applies to *free ports*³⁹ – special zones where goods (including those of high value, such as works of art) may be stored for an unlimited period, without the obligation to pay taxes or duties on this account. If the value of such transactions or several related transactions is at least EUR 10,000, the indicated entities are also treated as obligated institutions.

According to Statistics Poland data contained in the information on the activities of art galleries⁴⁰, as at the end of 2023,⁴¹ the aforementioned activities were carried out in Poland by 317 art galleries (compared to 310 in 2022).

³⁹ A free port is a kind of duty-free zone where goods, including those of high value, such as works of art, may be stored for an unlimited period, without the obligation to pay taxes or duties on this account. The best known free ports are located in Switzerland. The Financial Action Task Force states in its publications that free ports – due to insufficient security regulations, poor inspections and supervision – may be used for money laundering and financing of terrorist activities.

⁴⁰ <https://stat.gov.pl/obszary-tematyczne/kultura-turystyka-sport/kultura/rynek-dziel-sztuki-i-antykow-w-2023-roku,17,8.html>, access on 24.02.2025

⁴¹ Relevant Statistics Poland data for 2024 is not available.

3. INFORMATION ON DATA SUBMITTED TO THE GIFI

3.1. INFORMATION ON SUSPICIOUS TRANSACTIONS

In 2024, 8,129 suspicious activity reports (SAR), i.e. descriptive notifications of suspicious activities and transactions, were registered in the GIFI's IT system and used in ongoing analytical proceedings. The aforementioned notifications describe a few, several or even several hundred transactions (inter-related through parties thereto, circumstances in which a transaction was exercised, similar execution periods and/or involvement of the same assets) and their accompanying circumstances that according to the reporting institution/entity may be related to money laundering or financing of terrorism. These notifications often include additional data and documents substantiating the suspicion, and are aimed at facilitating the proceedings (e.g. account records, copies of the documents concerning transactions, etc.).

The extent of the information provided in the SAR has a direct impact on the GIFI's task completion time. The more information is provided in a notification, the more effectively it can be combined with data available to the GIFI and used in cooperation with the prosecutor's office and law enforcement agencies. Descriptive notifications may include, in particular, information on the reporting entity's suspicion that an offence has been committed, and on the accompanying circumstances. Table 3 presents information on the number of SARs received by type of reporting entity (2024 data shown against the data for previous years).

Table 3. Number of SARs received in 2001-2024

Period	Obligated institutions	Cooperating units	Other sources	Total
2001 (since July)	102	115	14	231
2002	358	237	19	614
2003	739	211	15	965
2004	860	521	16	1,397
2005	1,011	500	15	1,526
2006	1,351	530	17	1,898
2007	1,244	648	28	1,920
2008	1,287	460	68	1,815
2009	1,362	464	36	1,862
2010	1,462	476	59	1,997
2011	2,004	461	62	2,527
2012	1,954	436	37	2,427
2013	2,399	789	77	3,265
2014	2,739	823	75	3,637
2015	2,863	604	53	3,520
2016	3,290	853	55	4,198
2017	3,272	796	47	4,115
2018	2,982	543	97	3,622
2019	3,696	294	110	4,100

2020	3,587	179	39	3,805
2021	3,574	251	27	3,852
2022	4,280	208	17	4,505
2023	4,381	357	8	4,746
2024	7,635	484	10	8,129

The number of descriptive notifications registered in the system has remained in the range of approx. 3,400 to approx. 4,500 SARs/year for nearly a decade (Figure 3). In 2024, there was a 71% year-on-year steep increase in the number of SARs received, exceeding 8,000.

The source of the increase in the average number of SARs can most likely be attributed to the increasingly active analysis undertaken by obligated institutions, inter alia in connection with the GIFI's training activities (see Section 6.4). The above, at the same time, translates into increased awareness of obligated institutions.

Chart 3. The number of SARs received in 2006-2024

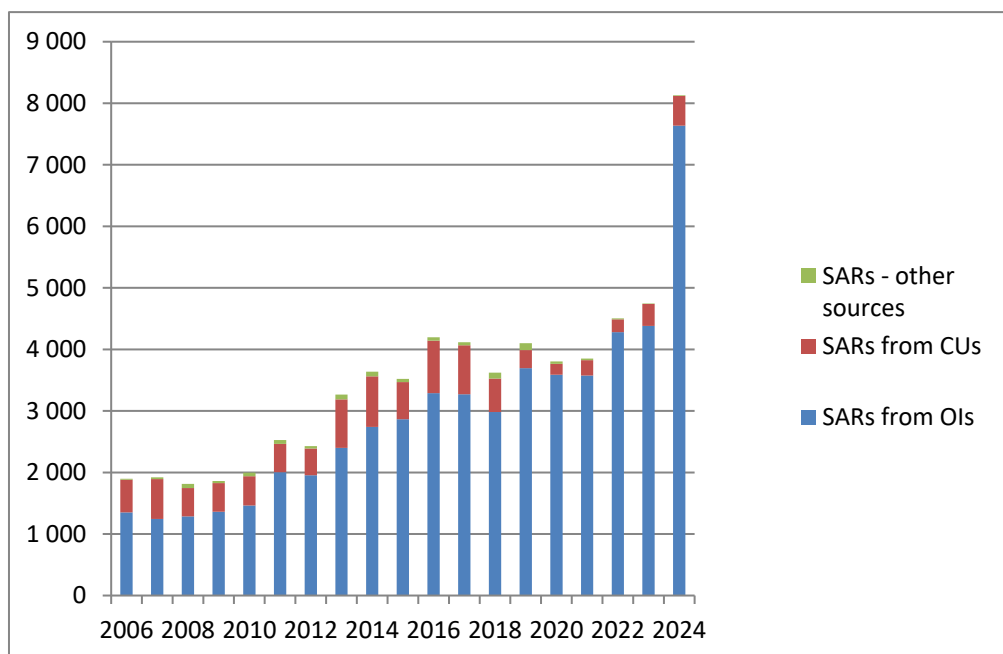
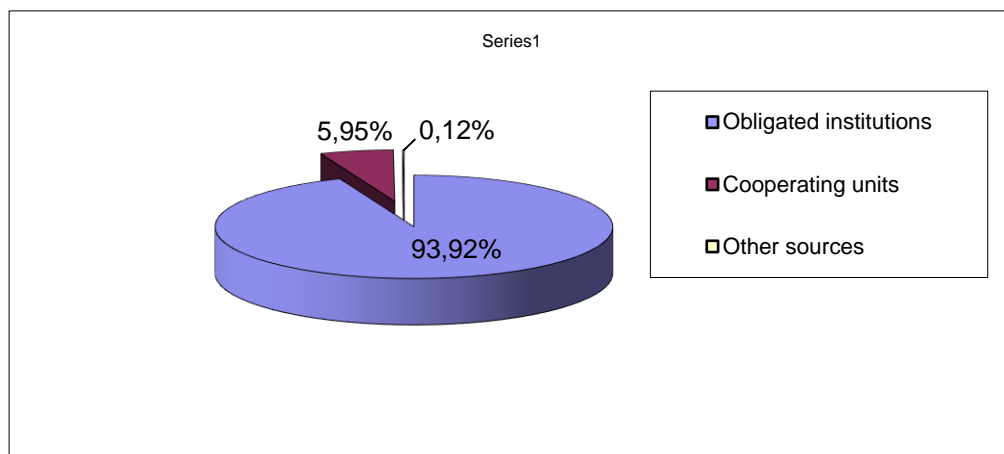


Chart 4 shows the percentage of descriptive notifications received from particular sources of information (a significant increase in the percentage of SARs from cooperating units).

Chart 4. Sources of SARs in 2024

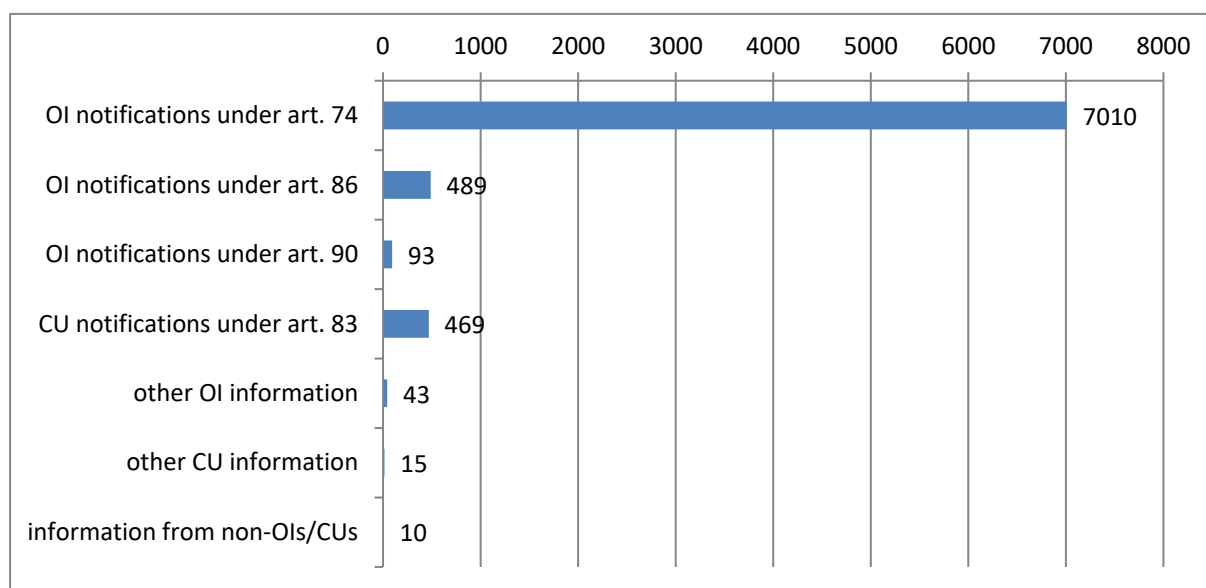


The total number of SARs registered in 2023 includes notifications and reports that differ depending on the circumstances of the events they concern, as well as the rationale and procedures for their submission to the GIFI. The applicable *AML/CFT Act* specifies – in the following articles:

- 74 (notification by an obligated institution of circumstances that may indicate a suspected offence of money laundering or financing of terrorism);
- 83 (notification by a cooperating unit of a suspected offence of money laundering or financing of terrorism);
- 86 (notification by an obligated institution of becoming aware of a reasonable suspicion that a specific transaction or specific assets may be related to money laundering or financing of terrorism);
- 90 (notification from an obligated institution of a transaction that the obligated institution reasonably suspects to be related to money laundering or financing of terrorism, where the submission of the notification prior to the transaction was impossible);

different rationale for submitting a SAR by an obligated institution or a cooperating unit to the GIFI. The numbers of different types of SARs registered by the GIFI in 2024 is shown in *Chart 5*.

Chart 5. Types of SARs in 2024

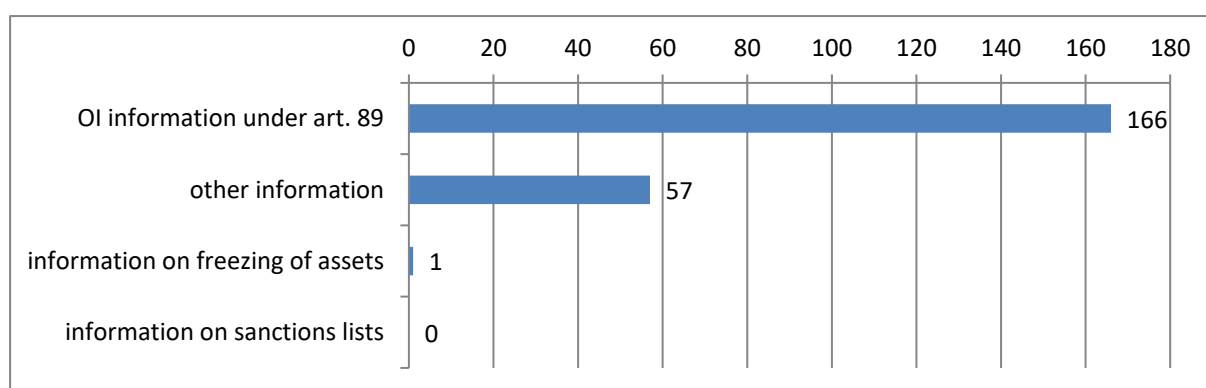


In 2024, 484 SARs from cooperating units (CUs) were registered, a further increase after almost doubling in number last year (357 in 2023 compared to 208 in 2022).

In 2024, the GIFI registered 7,010 SARs from obligated institutions. The significant increase in the information sent under Article 74 of the *AML/CFT Act* underlies the increase in the total number of SARs (as shown in Chart 3).

Besides SARs related to information on circumstances indicating a possible link with money laundering and/or financing of terrorism, the GIFI also receives other types of descriptive notifications that contain information on offences other than money laundering and/or financing of terrorism. The numbers of such notifications – that are included in ongoing analytical proceedings – registered in the GIFI’s ICT system in 2024 are presented in Chart 6.

Chart 6. Types of SARs concerning offences other than ML/TF in 2024



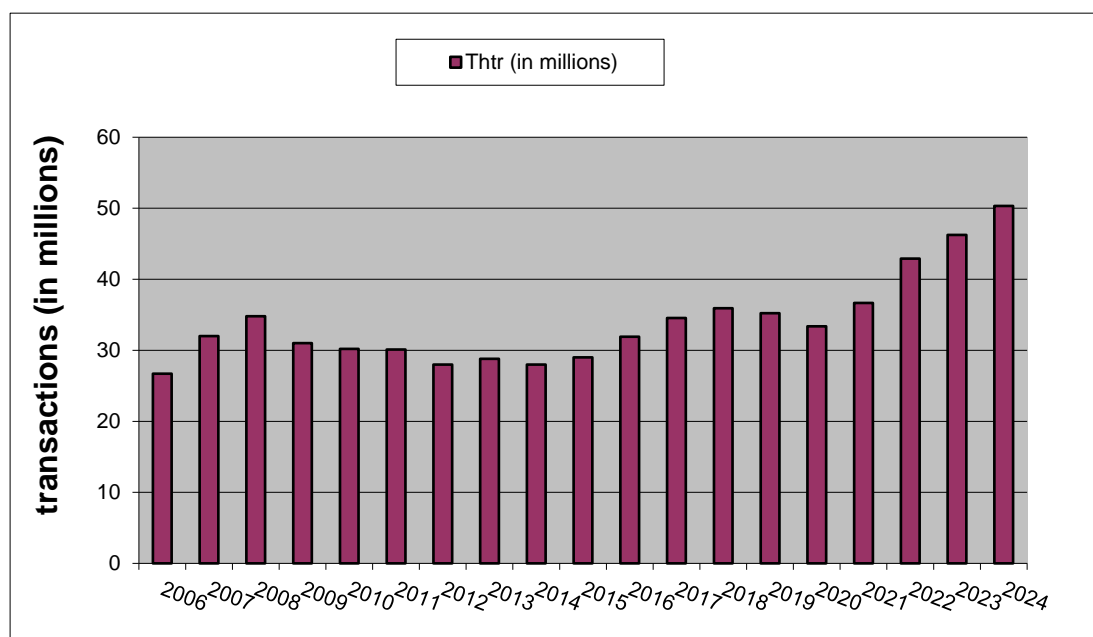
The number of registered descriptive notifications containing information on offences other than money laundering and/or financing of terrorism more than quadrupled (from 50 in 2023 to 224 in 2024), and the main increase concerned information addressed to the GIFI by obligated institutions under Article 89 of the *AML/CFT Act*.

3.2. INFORMATION ON ABOVE THRESHOLD TRANSACTIONS

In 2024, the GIFI received information on 50.34 million above threshold transactions reported under Article 72 of the *AML/CFT Act* (and additionally 270.2 thousand correcting reports – the large number of correcting reports was related to a mass action of sending corrections by one of the obligated institutions, which corrected previous reports after discovering a systematic error made when reporting information in previous years). This information is collected in the GIFI's IT system and processed by the Department of Financial Information in the Ministry of Finance – both for the purposes of analytical proceedings carried out by the GIFI and for the purposes of analyses carried out to respond to requests submitted by competent authorities. Information on aforementioned transactions, reported pursuant to Article 72 of the *AML/CFT Act*, is also made available in the source form to authorised bodies pursuant to the provisions of Article 105(2) of the *AML/CFT Act*.

The volume of information on transactions of this type submitted annually to the GIFI has been growing rapidly over the past few years (in 2024, the number increased by 37% from 2021 and, compared to 2023, – by 8,8%).

Chart 7. Volume of information on above threshold transactions received by the GIFI.



Obligated institutions submit data on the above-mentioned transactions in aggregate or separately, in the form of a file, on a continuous basis. Currently, all data is transferred electronically, and besides transfer through the GIFI's secure Internet website, which used to be the dominant method until 2018, the communication channel based on the network service of the ICT system of the GIFI, enabling the automation of the process on the part of the obligated institution, is widely used.

Transfer of information through the secure Internet website makes it possible both to send a file with information on multiple transactions, generated in a relevant format by the system of the obligated institution (this solution was used in the past mainly by large institutions that reported multiple transactions on a monthly basis, but these institutions currently use mostly a new

channel based on the network services of the GIFI's ICT system), and to complete a form (equivalent to an electronic document constituting a template of the electronic transaction card) directly on the Internet website (this solution is used mainly by smaller institutions that report few transactions on a monthly basis).

Out of the aforementioned 50.34 million transactions, information about which was submitted to the GIFI databases in 2024, 3.35% were transactions classified by obligated institutions as cash deposits or withdrawals. The year-on-year volume is again lower, as in previous years: 2020 (4.93%), 2021 (4.31%), 2022 (4.44%), 2023 (3.71%) . The only exception to the observed decreasing trend was a slight increase in 2022.

At the same time, 8.65% of transactions were classified by obligated institutions as coming from abroad, i.e. at a level comparable to the values for 2023 (8.10%) and 2022 (8.31% of all above threshold transactions).

The information obtained through the reports submitted under Article 72 of the *AML/CFT Act* provides insight into the structure of the information and its classification, which makes it possible to better assess the risk related to particular types of transactions, and also gives insight into important information (unavailable directly to the GIFI before 2020) on transactions particularly susceptible to ML/TF risks. This is enabled by, for example, categorisation of information on fund transfers. As for data reported since 2020, the GIFI obtained insight into the structure of the types of the process initiating funds transfers. For example, while in 2024 82.95% of outgoing transfers were initiated as a result of ordering a “traditional” credit transfer, the remaining 17.05% of above threshold transfers resulted from the execution of domestic or foreign money orders (8.27%) or from the execution of transfers initiated with the use of a payment card, electronic money instrument, mobile phone or other digital or IT device, or otherwise (8.78% in total).

The aforementioned 8.27% of above threshold transfers resulting from the execution of money orders in 2024 correspond to information on over 3,4 million money transfers. On the other hand, in the same data sample, the aforementioned 8.78% of above threshold transfers resulting from the execution of an order initiated with the use of a payment card, electronic money instrument, mobile phone, other digital or IT device, or otherwise, in 2024 correspond to information on more than 2,6 million funds transfers. The percentage share of the different groups of transfers related to remittances is very similar to that of the previous year, with the absolute numbers being higher due to an increase in the total number of transaction information reported.

A similar situation occurs thanks to the categorisation of information on incoming funds transfers from abroad. As for the reported data, the GIFI obtains not only information on more than twice as many transfers of this type than before 2020 (which are a group more susceptible to ML/TF risks than other transfers), but also an insight into the structure of the method of initiating a funds transfer. In 2024, 70.94% of above threshold transfers from abroad resulted from the execution of transfer orders, 11.90% of such transfers reached Polish obligated institutions as a result of the execution of money orders, and 17.16% of incoming transfers from abroad were classified by the receiving obligated institutions as resulting from the execution of a different type of order. In absolute numbers, this corresponds to, respectively, over 3 million transfers from abroad, over 518 thousand remittances from abroad, and over 747 thousand fund transfers from abroad of other type.

The indicated absolute volumes of various types of information show, on the one hand, the scale of the issue related to the efficient combination of collected information with other data sources, and, on the other hand, demonstrate the ability to differentiate procedures for information classified to different risk areas; currently this is possible for all information on transactions entering the GIFI's ICT system.

The received information on transactions was made available in the ICT system of the GIFI as input data for further analyses. In particular, this information was subjected to automatic analytical processes. For example, all information on transactions was verified for possible links with entities suspected of financing of terrorism or entities from high-risk/sanctioned countries. Links between information on transactions and other types of information available in the system (e.g. with enquiries of external entities – a prosecutor's office, foreign FIUs, etc.) are automatically searched for, to be then used in analytical proceedings or to be transferred to external entities (as a response to a request for information or on the GIFI's initiative). The above-mentioned links were searched for with the use of the analytical models available in the ICT system of the GIFI, to be used both in the processes of automatic report generation and in *ad hoc* analyses for the purposes of a specific problem.

Information on above threshold transactions is used both for the extraction of data on transactions and entities involved in them, being a helpful source of data used in analytical proceedings, and for the extraction of additional information on suspicious entities (bank accounts, related entities, etc.). Information on transactions is available for analysis both in a simple form, where by asking a question about a specific entity or account, it is possible to access the collected data, and as the source for the analysis of links – by using the possibility to search the database for related objects (bank accounts, entities), i.e. those being in a defined type of relationship (e.g. entities or bank accounts linked through occurrences in the transaction chain).

.

4. ANALYSES

4.1. COUNTERACTING MONEY LAUNDERING

Obtaining, collecting, processing and analysing information in accordance with the provisions of the *AML/CFT Act* and taking action to counteract money laundering and financing of terrorism is the basic task of the GIFI. When performing this task, the GIFI investigates the course of transactions with respect to which it has a reasonable suspicion of a violation of the law. Moreover, it provides authorised entities with information about transactions, and obtains requested information from obligated institutions, as well as cooperates with foreign institutions and international organisations dealing with counteracting money laundering or financing of terrorism. All the above mentioned activities are undertaken in order to conduct comprehensive analysis of the collected information in terms of ML/TF offences that could have been committed by suspected entities. The analysis is aimed at substantiating that assets subject to the respective transactions originate from proceeds from a prohibited act.

4.1.1. ANALYTICAL PROCEEDINGS AND THEIR EFFECTS

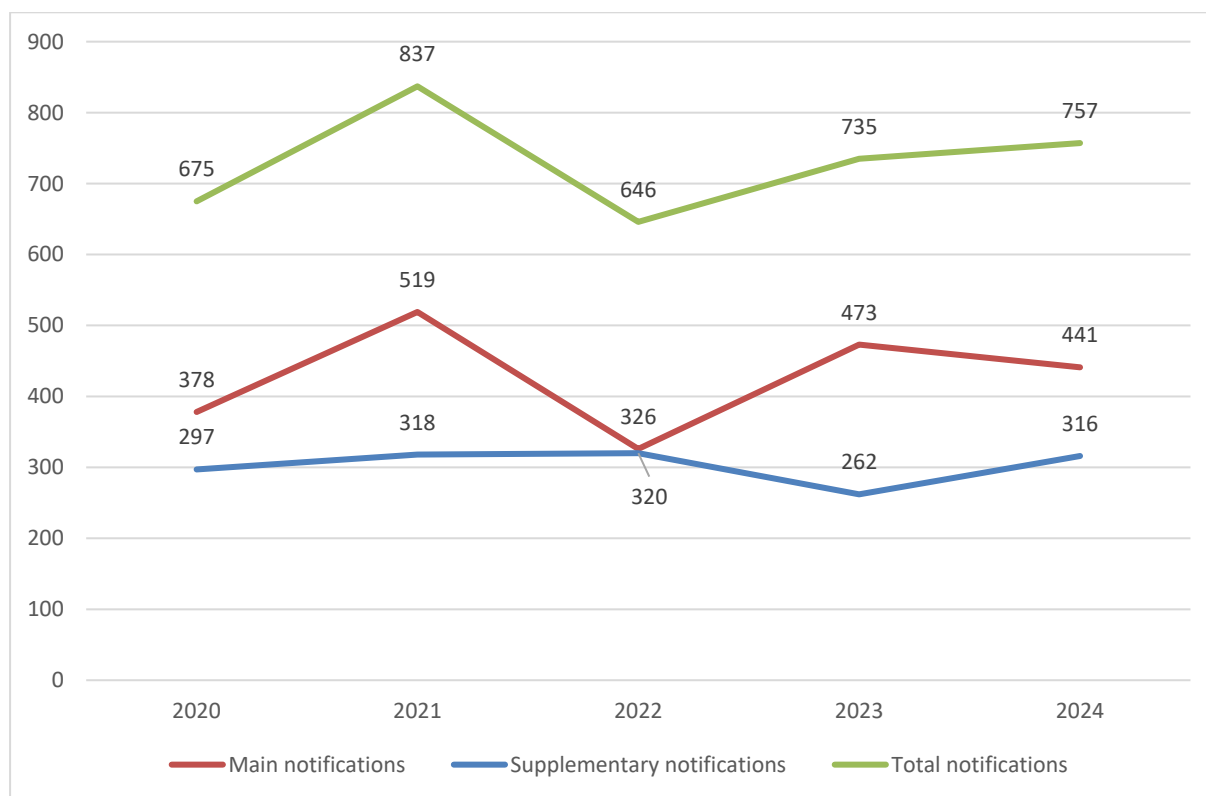
In 2024, the GIFI initiated 4,765 analytical proceedings regarding suspected money laundering or financing of terrorism. Compared to 2023, the number of initiated proceedings increased by approx. 38,4%.

As a result of its analyses, in 2024 the GIFI submitted a total of 757 notifications to prosecutors' offices. Compared to 2023, when the total number of notifications was 735, there was an increase by approx. 3.0%.

The total of 757 notifications submitted to prosecutors' offices in 2024 includes 441 notifications of suspected money laundering offences (so-called main notifications). Compared to 2023, there was a decrease of *approx.* 6.8 % in the number of main notifications sent to the prosecutor's office. The amount of assets covered by the main notifications submitted to the prosecutors' offices in 2024, converted into PLN, was more than PLN 5.21 billion, a decrease of approx. 45.8 % compared to the previous year.

Having submitted a notification on a suspected money laundering offence, the GIFI most often obtains and processes additional information on previous or subsequent transactions carried out by entities and persons whose activities were covered by the main notification, requests data from foreign FIUs or additional information on trading partners or related entities. The collected materials and the findings of additional analyses are submitted to the prosecutor's office as so-called supplementary notifications. In 2024, the GIFI prepared 316 such notifications (i.e. approx. 20.6 % more than in the previous year, when the number was 262). The total assets that were the subject of suspected offences in the supplementary notifications amounted to approx. PLN 160 million.

Chart 8. Numbers of notifications submitted to the prosecutor's office and notifications submitted to 49 cooperating units in 2020-2024



Source: the GIFI's own data; as at 12 March 2025

Approx. 62.1% of the number of main notifications concerned suspected money laundering involving proceeds related to various types of fraud and deception, approx. 33.6% – fiscal offences, and approx. 12.2% of the notifications concerned the activities of organised crime groups (see Chart 8).

It should concomitantly be emphasised that the GIFI's notifications may concern several predicate offences. According to the GIFI, the first of these groups includes offences relating to:

- investment, consisting in making natural persons, often foreigners, unfavourably dispose of property by offering these persons fictitious investment, mainly in cryptocurrencies;
- impersonating another person or a trading partner and persuading mainly businesses to order payments to fraudsters' accounts;
- phishing to obtain data enabling access to financial products or other confidential information enabling fund theft.

The latter group covers all types of fiscal offences, including VAT fraud.

Chart 9. Percentage of the most common predicate offences in the GIFI's notifications in 2024 (by the total number of notifications with a specific case typology)



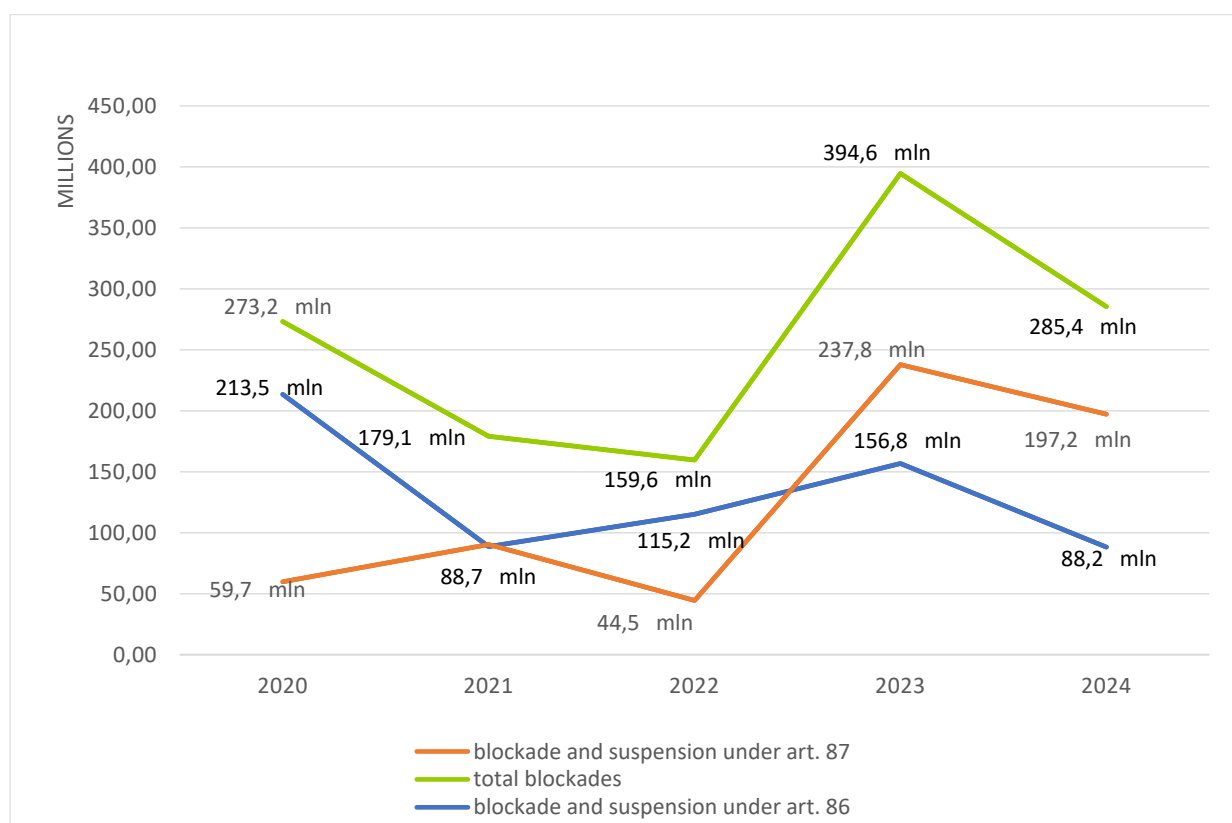
Source: the GIFI's own data; as at 20 March 2025

Having received notifications from obligated institutions pursuant to Article 86 of the *AML/CFT Act*, the GIFI blocked 413 accounts with funds with a total value of approx. PLN 84.0 million⁴² and suspended 105 transactions for a total amount of approx. PLN 4.2 million. The value of such blocked accounts decreased by approx. 44.9 % compared to 2023, with an approx. 39.2 % decrease in the number of blocked accounts (in 2023, there were 679 blocked accounts). The value of the suspended transactions was 4.2 million, which represents an approximate 2.9 % reduction in this amount, with an approx. 101.9 % increase in their number (in 2023, there were 52 suspended transactions).

In 2024, the GIFI, on its own initiative, blocked 641 accounts with a total balance of approx. PLN 148.5 million and suspended 17 transactions for the total amount of approx. PLN 48,7 million. The value of account blockades decreased by 34.8%, compared to 2023, with an approx. 39.0% increase in their number. The value of suspended transactions in 2024 increased by approx. 388.0%, with an approx. 142.9% increase in their number.

⁴² The amounts of funds in blocked accounts are estimated ones and their actual amount may be higher due to the specific characteristics of account blocking – while an account remains blocked by the GIFI, it can still be credited, but it is not possible to withdraw or transfer funds deposited in it to other accounts.

Chart 10. Value of account blockades and transaction suspensions in 2020-2023 (in PLN million)



Source: the GIFI's own data; as at 12 March 2025

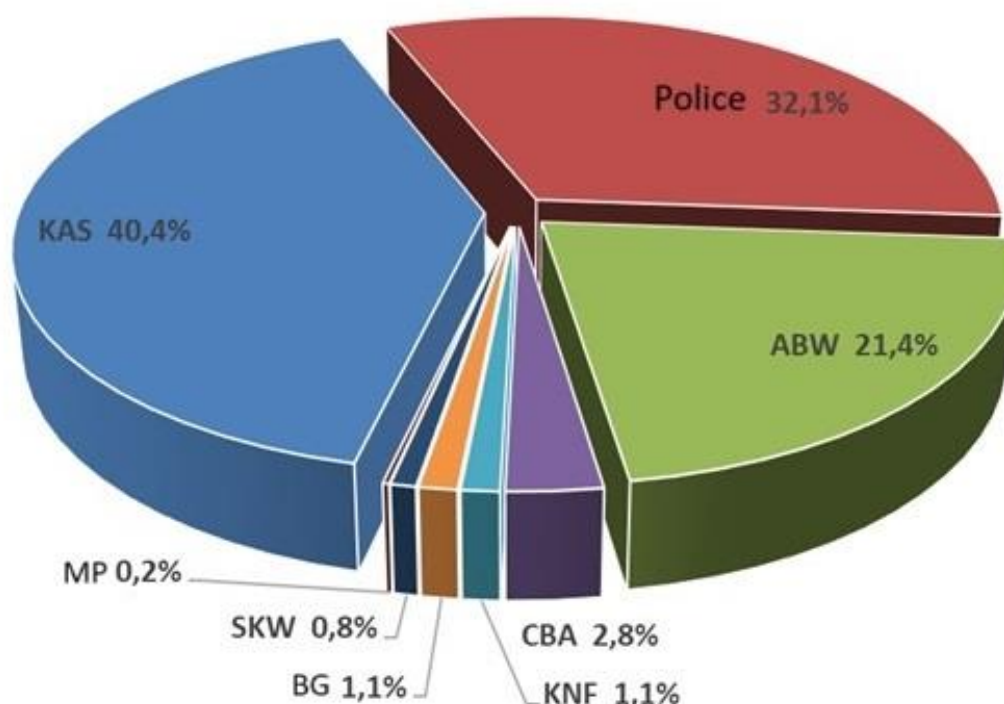
The GIFI submitted 532 notifications to the authorised bodies (i.e. in the manner specified in Article 106(1) or (1a) of the AML/CFT Act).

Table 4. Numbers of notifications submitted to the authorised bodies in 2024

Cooperating units	Number of notifications
National Revenue Administration (KAS)	215
Police	171
Internal Security Agency (ABW)	114
Central Anti-Corruption Bureau (CBA)	15
Polish Financial Supervision Authority (KNF)	6
Border Guard (BG)	6
Military Counter-Intelligence Service (SKW)	4
Military Police (ŻW)	1

In 2024, the greatest numbers of the GIFI's notifications were addressed to the KAS bodies (approx. 40.4%) and the Police bodies (approx. 32.1%). The GIFI informs the central Police authorities of suspected offences other than money laundering and financing of terrorism. Most of the notifications sent to the KAS bodies concern suspected fiscal offences related to VAT. The other notifications contain information regarding suspicions of concealing the object of taxation, understatement of revenue, undisclosed income or fiscal offences related to goods imports.

Chart 11. Percentage of notifications sent by the GIFI by cooperating units



Source: the GIFI's own data; as at 12 March 2025

In 2024, the largest number of notifications were sent by the GIFI on its own initiative to the KAS bodies (see Chart 12). As in the previous years, the overwhelming majority of these notifications concerned suspicions of various fiscal offences related to VAT, including understatement or failure to disclose turnover through forging or concealing invoices, input VAT fraud, “missing trader” fraud, carousel fraud, and intracommunity transactions. Some of the notifications contained information regarding suspicions of concealing the object of taxation, understatement of revenue, undisclosed income or fraud in the import of goods. The notifications also concerned violations of compliance with restrictive measures set out in separate legislation introduced in response to Russia's aggression against Ukraine.

The notifications submitted by the GIFI to the National Revenue Administration bodies were often used by these bodies to initiate control proceedings to verify the correctness of calculation and payment of taxes being the State budget income from personal income tax, corporate income tax and value added tax. The findings of control proceedings repeatedly showed that the controlled entities did not conduct the actual declared economic activity and were issuing “blank” VAT invoices that were then used by buyers to unduly diminish output VAT, which depleted the amounts due to the State Treasury. Furthermore, the aforementioned control proceedings indicated that the controlled entities did not pay VAT amounts to the competent tax office, as demonstrated on sale invoices they issued. The findings of the control proceedings and the collected evidence were used to initiate investigations into fiscal offences, that were then transformed into investigations conducted under the supervision of prosecutors' offices. As a result of the coordination of actions taken, the GIFI participated in such prosecutors' investigations, providing evidence consisting of the analyses of financial flows, and blocked

accounts where it could reasonably suspect that the identified assets originated from proceeds from a prohibited act.

The GIFI also provided a significant number of notifications to the Police, including the Central Investigation Bureau of the Police (CBŚP). The information contained in those notifications was used by the aforementioned cooperating units to undertake their statutory activities that resulted, among others, in instigating preparatory proceedings. The information submitted by the GIFI was also used in pending proceedings.

Another large group of notifications contained information provided to the Internal Security Agency (ABW). Those notifications included data regarding transactions that could be related to a suspicion of a prohibited act, the examination of which falls within the competence of the Agency, including identifying, preventing and detecting offences against the economic foundations of the state and its security, identifying, preventing and detecting any acts of corrupting public servants, and any offences concerning manufacture of or trading in goods, technologies and services that are of strategic importance for the security of the state, illegal production or possession of and trade in weapons, ammunitions and explosives, weapons of mass destruction as well as intoxicants and psychotropic substances in international trade.

Notifications including a comprehensive analysis of suspicious and economically unjustified financial flows submitted by the GIFI on its own initiative, following their verification and completion of their statutory activities by law enforcement agencies, constituted comprehensive evidence providing sufficient grounds for the initiation of an investigation or were incorporated into pending criminal proceedings. The information sent by the GIFI was also repeatedly used by prosecutors to prepare written requests to the GIFI for disclosure of information collected in accordance with the procedure and within the scope provided for in the Act for the purposes of pending criminal proceedings. Preparatory proceedings carried out in connection with the notifications sent by the GIFI made it possible to present charges of committing an offence to a number of people and to recover assets worth many million. In many cases, the coordination of activities carried out by the GIFI and the competent law enforcement agencies made it possible to arrest members of criminal groups and block bank accounts with assets derived from proceeds from prohibited acts.

In addition, the GIFI has planned ten themes for strategic and/or sectoral analyses for 2024, of which nine themes have been undertaken and three have been completed. The others are being continued in 2025.

4.1.2. EXAMPLES OF ANALYSIS DIRECTIONS (INCLUDING SANITISED CASES)

Laundering of money derived from the fraudulent acquisition of European Union funds for the construction of photovoltaic farms

The GIFI received information from one of the cooperating units that the owner of several companies grants them multi-million loans despite having little income from the pension she receives. The above-mentioned companies have received EU funding for the construction of several photovoltaic farms. An analysis of the flow of funds found that EU funding had been granted on the basis of documents certifying untruth (bank account balances indicating funds held for the own contribution had been artificially generated) submitted by the companies. Consequently, if the companies had submitted documents showing the actual balances, they

would most likely not have received EU funding. Subsequently, the funding obtained was used for investments related to the construction of farms of entities related by persons and capital to the companies analysed, which is not in line with the rules on the award of EU-funded contracts.

The reliability of the cost estimates of the budgets attached to the funding applications was also questionable. An analysis of the flow of funds showed that, in fact, in each of the projects, the own contribution came from the procurement contractor and it can be assumed that the budgets of the projects were significantly inflated so that there was no real need for own contributions, which the companies did not have.

In addition, it was found that the companies in question had received investment loans from banks for the construction of photovoltaic farms, which had already been built and paid for with EU funding. The funds from the loans were mostly used for the day-to-day operations of the related company.

Once the photovoltaic farms were operational, the income generated was used, among other things, for expenses related to the companies' day-to-day operations and as loans and dividends transferred to the owner's accounts. Subsequently, the funds were transferred to an immediate family member as a donation, for which, among other things, real estate was purchased. At the same time, it was established that, in reality, the companies were managed by the above-mentioned immediate family member, and their owner was probably a so-called "money mule".

On the basis of the collected information, the GIFI decided to submit a notification to the prosecutor's office.

Laundering of money derived from defrauding the National Centre for Research and Development (NCBR) of European Union funding

The GIFI has received information from the obligated institution that a group of individual and corporate clients are linked to individuals suspected of fraudulent acquisition of EU funding in 2021-2023 allocated by the NCBR.

In the course of the analysis of the flow of funds it was established that the EU funding provided by NCBR for the implementation of project X (establishment of a Fund, providing grants for the implementation of innovative B+R projects) was received on the basis of documents certifying untruth – the beneficiary in fact did not have an own contribution (part of the bank account balances indicating funds held for the own contribution had been artificially generated). Therefore, if the beneficiary had provided documents with the actual balances, they would most likely not have received EU funding. In addition, the own contribution actually came from public and not private funds.

At the same time, it has been established that it was most likely the intention of the applicants from the outset to plan and implement the project in such a way as to control all the funds transferred to the grantees and to be able to transfer them to other related companies and then, through subsequent transactions, to transfer them to the accounts of foreign related entities. This was indicated by:

- the transfer of grants to companies set up by persons related to the beneficiary, who probably acted as so-called "money mules", and the payment for this was most likely the remuneration paid as part of the implementation of the projects,

- the subject matter of the B+R projects was consistent with the activities of the subcontractors related to the beneficiary,
- the Fund's managers had powers of attorney over bank accounts belonging to some of the grantee companies,
- accounting services were handled by the same company in most of the companies (probable coordination of the flow of funds between the grantee companies and the subcontractors),
- funds received from grants were mostly transferred to companies related to the Fund's managers,
- the obfuscation of the transfer of funds between accounts took place through the purchase and sale of many bills of exchange between the grantee companies and the subcontractors and foreign companies,
- a semblance of real project implementation was maintained by allocating small amounts of funds to entities and individuals who carried out real business activities and performed the commissioned tasks to a sufficient extent so that the grantees could "account" for the funds received and demonstrate the implementation of the B+R projects,
- the suspension of the activities of most grantee companies at the end of its implementation.

In addition, because the invoices issued under the grants received were unlikely to reflect true business events or may have been significantly overstated, the grantee companies recovered undue VAT refunds.

On the basis of the collected information, the GIFI decided to submit a notification to the prosecutor's office.

Laundering of money derived from overpricing in tenders for the military

The GIFI has received information from a foreign FIU about the probable involvement of an entity registered in Poland in the transfer of funds that may originate from a prohibited act of overpricing in tenders for the military.

In the course of the analysis, it was established that the account of a limited liability company whose beneficial owner was a foreigner showed a pattern of transactions consisting of incoming transfers from abroad with titles of payment for invoices, followed in quick succession by transfers of funds to southern European companies. The southern European companies were allegedly engaged in logistics activities.

Among other things, attention was drawn to the initial dormancy of the account and the absence of transactions typical of business operations. Furthermore, as part of the application of customer due diligence measures, the obligated institution asked the client to provide documents justifying the transactions in its accounts. The company provided documents showing that the goods it sold were transported from Warsaw. However, there were no transactions on the company's accounts indicating ownership or rental of warehouse space.

On the basis of the collected information, the GIFI decided to block the company's accounts and to submit a notification to the prosecutor's office.

Laundering of money derived from violations of sanctions imposed on Belarus (EU Council Regulation 2024/1865 of 29 June 2024) in connection with the export of passenger cars to third countries

Since Russia's invasion of Ukraine began on 24 February 2022, the European Union has imposed sanctions on the Russian Federation in addition to earlier sanctions imposed since 2014 in connection with the annexation of Crimea and the failure to implement the Minsk agreements. As part of the economic sanctions, the EU has introduced a number of import and export restrictions against Russia. Due to the close economic integration of Russia and Belarus, which made it much easier to circumvent the sanctions in place against Russia, EU Council Regulation 2024/1865 of 29 June 2024⁴³ – which in turn amended EC Council Regulation 765/2006 of 18 May 2006⁴⁴ – came into force on 1 July 2024; this Regulation extended and tightened the existing rules and introduced new sanctions against Belarus due to its involvement in the Russian aggression against Ukraine. According to the above regulation, the sale, supply, transfer or export, directly or indirectly, of luxury goods, whether or not originating in the Union, to any natural or legal person, entity or body in Belarus or for use in Belarus was prohibited. Thus, the ban extended to the export of passenger cars classified as luxury goods and vehicles that can be used to support strategic or military activities.

The analytical case involved two Polish limited liability companies and one foreign company. All of those entities were managed by the same person.

The analysis found that the companies were primarily engaged in the luxury car trade. The main principal for the funds credited to the companies' accounts was a Belarusian entity. The Polish companies purchased vehicles mainly from European counterparties, while the foreign company purchased cars from Polish entities. Despite the entry into force of the regulations related to the imposition of sanctions on Belarus, the pattern of the flow of funds in the companies' accounts did not change. Both before and after 1 July 2024, the main contributor was a Belarusian entity. At the same time, from that period onwards, Polish companies stopped showing exports of goods from the territory of Poland to the eastern counterparty in their declarations and started declaring sales to other entities from Eurasia. The GIF's findings show that transactions made on the companies' accounts, after 1 July 2024, are carried out mainly on the basis of trilateral agreements, in which the payer is an entity from Belarus, while the recipient of goods and the ordering party is allegedly a company from Eurasia.

An analysis of transactions in the companies' accounts showed that in the description of incoming transfers, the CN code for vehicles up to 1,500 cc appears most frequently. This code is not included in Annex XXII issued to Council Regulation (EU) No 833/2014⁴⁵ concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, which means that, inter alia, the sale, supply or transfer of these goods to Russia is not prohibited. At the same time, on the basis of the information available, it was established that the main object

⁴³ Council Regulation (EU) 2024/1865 of 29 June 2024 amending Regulation (EC) No 765/2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine

⁴⁴ Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine

⁴⁵ Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine

of the transaction are vehicles with a cubic capacity exceeding 1,500 cc, which means that these goods are covered by the sanctions imposed on Russia and Belarus and are discrepant with the CN codes⁴⁶ indicated by the payer in the titles of the transfers.

On the basis of the collected information, the GIFI decided to block the companies' accounts and to submit notifications to the prosecutor's office.

Laundering of money derived from financial gains from betting as part of a special offer for new players using phished personal details

The GIFI received a notification from an obligated institution informing it that transfers from a betting company were made to numerous savings accounts (approx. 1,300) established in the name of Mr. X. Each time, a different third party unrelated to the owner of the accounts was entered as the recipient of the funds. The funds were then transferred to one main account and the savings account was closed.

In the course of analysing the flow of funds, it was established that the fraud scheme consisted of setting up as many player accounts as possible with different personal details and assigning bank accounts to them, which were owned by one person. In total, Mr X set up 3,185 player accounts with different personal details. The purpose of the above was to take advantage of the opportunity to place bets with the betting company as part of an offer aimed at new players (and one player account). The special offer consisted of risk-free betting and, in the event of a losing bet, a refund of the deposited amount to the player's account. Once the bets had been placed, the funds in each player's account (winnings and funds refunded by the betting company in the event of losing bets) were transferred to the bank account assigned to the account. The funds from these accounts were then immediately transferred to one of several accounts belonging to Mr X, which he partly further deposited as new bets on new player accounts, paid out in cash, and also transferred to telephones as likely payment for the use of the details to set up a player account.

It was established that Mr X was most likely paying for scans of identity cards and that the sale and purchase of identity documents was taking place over the Internet. In addition, player accounts were also set up with the details of family members, whose children/siblings most likely were the ones who received funds from Mr X via a blik transfer to their phone. This may indicate that they were providing scans of their parents' / other family members' identity documents, and the fact that they were being paid for this suggests that they may have been doing this without the knowledge of the document owners.

On the basis of the information gathered, the GIFI decided to block Mr X's accounts and to submit a notification to the prosecutor's office.

Laundering of money derived from the organisation of collective participation in games of chance contrary to the provisions of the Act of 19 November 2009 on Gambling

Personally related limited liability companies with minimum share capital organised 'promotional lotteries' throughout Poland. The promotional products in the lotteries were

⁴⁶ CN codes are a structured classification of goods created for customs purposes, which organises all goods in circulation.

e-books and their purchase entitled the holder to receive lottery tickets. The e-books were available in several versions and for each version a corresponding number of lottery tickets was assigned (from 1 to 10 tickets). The price paid by the person participating in the lottery depended on the number of lottery tickets sold together with the e-book. The e-books themselves, on the other hand, were only available during the "promotional lottery" period and it was not possible to purchase the publications either before or after the lottery. At the same time, it was not possible to purchase the e-book without agreeing to participate in the lottery. This was followed by a prize draw on a date set by the organiser, usually on the YouTube platform. The prize draw hosts were well-known influencers from the world of social media. The very purpose of the promotional lottery also seemed to be unfulfilled. The purpose of the promotional lottery was ostensibly to promote a product, service or venture. However, it is likely that the organisers' actual aim was to make a profit from the sale of the lottery tickets, with promotion of the product being a side issue and the least important one. This gave rise to the assumption that the e-books themselves were a means of raising revenue from the sale of lottery tickets. The sale of the e-book itself as a product was less important, as the purchaser was focused on the add-on to this product, i.e. the ticket entitling them to enter the draw for attractive prizes.

An analysis of the accounts held on behalf of these companies showed that between October 2021 and October 2024, they had accumulated funds totalling more than PLN 320 million, which came from payments made by various natural persons through online payment systems offered by various payment institutions. These were payments for lottery tickets offered under the guise of selling and promoting e-books. The funds raised in this way were then transferred, with titles indicating payment of invoices to influencers (including businesses owned by them) for whom the lotteries were organised, or used to pay dividends of several million PLN to the shareholders of the companies organising the lotteries and to grant sham loans to various entities. In addition, funds in the amount of PLN 61 million were invested in a company, one of whose owners was a well-known influencer. This amount represented two-thirds of the company's revenue during its period of operation. One of the persons who generated revenue from the organised lotteries transferred part of the funds received to a non-European country, with titles indicating the purchase of a house and a car, and invested it in a restaurant.

An analysis of the circumstances of conducting promotional lotteries based on the sale of e-books using the image of well-known influencers and the flows in the accounts led to the suspicion that the organisers of the lotteries may have acted contrary to the provisions of the *Act on Gambling* and, under the guise of organising promotional lotteries, actually conducted gambling or other games of chance not classified in the Act, the purpose of which was the sale of tickets rather than the promotion and sale of e-books. At the same time, taking advantage of the current legal system, the organisers obtained tax-free income from the organised lotteries, bearing only the burden of 5% VAT on the sale of e-books. In addition, the entities involved declared their purchases and sales to each other, which could indicate that these transactions were a sham by issuing VAT invoices that were unreliable and certifying untruth in terms of legal and factual circumstances. They were relevant to the determination of the amount of the public liabilities and misleading the tax authorities in order to avoid payment and reduce the public tax liabilities due to the State Treasury.

On the basis of the collected information, the GIFI decided to block funds in the total amount of approx. PLN 107 million, accumulated on the accounts of the entities covered by the analysis, and to submit a notification to the prosecutor's office.

Laundering of money using an account held in the name of a Polish user for fraud linked to the collapse of a global cryptocurrency exchange

Analytical case initiated on the basis of a notification from an obligated institution providing virtual currency exchange services.

The Polish user's account saw a number of incoming transactions for large sums of money, then the funds raised were transferred to a cryptocurrency exchange and private wallets. An analysis by the aforementioned institution showed that the account user initially logged in from a Polish IP address and used Polish language settings, but with increased activity on the account, a change of language to English and the use of a VPN was observed, as well as the use of a time zone for a country located in southern Asia and the Indian Ocean.

The above information coincided with information regarding fraud on a global cryptocurrency exchange and a lawsuit filed by the exchange against a cryptocurrency trader from the aforementioned region of the world for orchestrating massive market manipulation - using stolen identities, as a result of which the cryptocurrency exchange was defrauded of USD 1 billion.

The above-mentioned Polish account user was most likely linked to criminal groups operating in Poland, among others, as well as extremist groups potentially linked to terrorist financing.

At the same time, the provider of virtual currency exchange services has received enquiries and requests from foreign law enforcement agencies regarding the account of the Polish user.

In the course of the analysis carried out by the GIFI, it was established that the bank accounts held in the name of the Polish citizen did not show transfers of significant amounts. The above-mentioned user also had no savings and did not declare income/revenue to the tax authorities which could indicate that he may be in possession of millions of USD.

On the basis of the collected information, the GIFI decided to block the user's accounts and to submit a notification to the prosecutor's office.

Laundering of money derived from stolen crypto-assets from foreign cryptocurrency exchanges at a Polish obligated institution

A citizen of an Asian country, posing as a representative of a Middle Eastern company, electronically concluded an agreement to exchange 10 BTC for USD with a Polish obligated institution providing virtual currency services. The bitcoins allegedly came from payments for two luxury watches sold by the Middle Eastern company.

After signing the agreement, the aforementioned person transferred the bitcoins to the obligated institution's address, but used a different own address for this purpose than the one indicated in the agreement. The obligated institution conducted an analysis of the public register of BTC transactions and found that the address from which the funds were sent had indirect exposure to an address on the OFAC SDN sanctions list and was flagged as an address controlled by a known hacker group.

The above-mentioned group is made up of hackers accused of having links to the North Korean government. This group is believed to have stolen more than 1,500 BTC from various institutions around the world. The funds that were transferred to the wallet of the Polish obligated institution came from the theft of crypto-assets from popular cryptocurrency exchanges/platforms.

The client of the obligated institution presented various documents that purported to prove the legitimate origin of the funds, including an authorisation to enter into trade agreements on behalf of the said Middle Eastern company, an invoice for the watches, a scan of their passport and even a scan of the passport of their counterparty, which in itself constituted a suspicious circumstance. The authenticity of these documents was questionable. Essential information was missing from the invoices. The address of the Middle Eastern company indicated in the documents did not match the address that was listed on the company's website. The website offered sparse information and did not show that the company specialised in the sale of luxury watches.

The GIFI's analysis confirmed that the obligated institution's client address received funds from more than one address attributed to the aforementioned hacker group. This was an argument reinforcing the suspicion that the owner of the address knew their origin and was not selling watches at all, while their task was to check the possibility of exchanging stolen bitcoins for FIAT currency at the Polish obligated institution. However, the latter correctly applied customer due diligence measures and detected the attempted money laundering, as a result of which the funds were blocked and a notification was sent to the relevant prosecutor's office.

Laundering of money derived from the gains of impersonating a foreign company

The GIFI received a notification from an obligated institution that a Polish limited liability company, presumably in order to obtain financial gains related to extortion of funds, 'impersonated' an EU company that had been operating in the construction industry for many years and, a few days before receiving a transfer from a Swiss account held for an overseas company as payment for an invoice, changed the name of its company to coincide with the name of the aforementioned EU company.

After receiving funds from the overseas company to its bank account indicating payment for invoices issued, the Polish company transferred part of the funds to the private accounts of its shareholders, part to a foreign account as payment for an invoice, and a significant part to a cryptocurrency exchange service provider.

The purpose of the purchase of the virtual currency (USDT⁴⁷) was, in turn, to pay an invoice issued by an Asian entity for photovoltaic panels to be used, according to an investment agreement with a Panamanian company, in a shrimp farming project to reduce energy and electricity costs.

An analysis of the bank accounts and the facts of the case indicated that both the investment agreement and other documents had been created by the Polish company for the sole purpose of lending credence to the legality of the transactions carried out. All actions taken by the Polish company (purchase of shares in an existing company, change of name to a name similar to that of the EU company, opening of accounts in a Polish bank, acceptance of funds into the account

⁴⁷ USDT - an Ethereum token that is pegged to the value of the US dollar (also known as stablecoin)

from a Swiss account belonging to an overseas company, exchange of currency into virtual currency) were aimed at thwarting or significantly hindering discovery of the criminal origin of the funds accepted into the bank account. The funds were likely to have originated from financial fraud.

On the basis of the information gathered, the GIFI decided to block the funds collected on the bank account, to suspend the purchase transaction of virtual currency by the Polish company, and to submit a notification to the prosecutor's office.

Laundering of money derived from trading in unregistered shares of the company

Analytical case initiated based on a notification from an obligated institution maintaining the Shareholders' Register of the Company (not listed on the Stock Exchange).

The institution identified a pattern of behaviour among the Company's shareholders which consisted in concluding Agreements for the sale of non-existent "X" series shares; these transactions were reported to the institution by the persons acquiring these blocks of shares in order to make the relevant annotations in the Company's Shareholders' Register.

In the course of the analysis, the notifying party noted that the registry court having jurisdiction over the Company had not yet had time to register the assumed increase in the Company's share capital in the National Court Register, while these unissued shares were already subject to secondary trading, as if the rights attached to these shares already existed and as if their transfer could take place on the same basis as in the case of duly issued, registered and recorded shares of previous issues.

The suspicions were confirmed during the analysis of the Company's annual financial statements for recent years. None of these statements disclosed the "X" series shares which, in the opinion of the GIFI, were subject to fictitious trading.

At the same time, an analysis of the financial flows in the account of the Seller (a well-known stock exchange investor) revealed several incoming transfers totalling more than PLN 2 million from the Buyers. The titles of the transactions indicated payments under agreements for the sale of the Company's shares from particular days or concerning a specific number of shares (without indicating which specific series of shares were the subject of the transactions). Based on a comparison of the sales agreements submitted by the obligated institution and the requests for entry in the Shareholders' Register, it was possible to link the actual transfers with fictitious agreements for the sale of non-existent shares.

In view of the possible violation of regulations related to the operation of the financial market, the case was referred to the competent authorities according to the jurisdiction.

Laundering of money derived from the transfer of investment fraud funds

The case involved three limited liability companies, with minimum share capital, registered a few days apart from each other, based in the same virtual office. The sole shareholder of these companies was the same person.

The accounts of these companies held in Polish banks received approx. EUR 600 thousand within two months of their establishment. The senders were several hundred natural persons, mainly from two EU countries.

Most of the funds received were immediately transferred to accounts held in the European Union and Asia. Some of the funds, in the form of a series of low-value transfers, were transferred to accounts held in European Union countries, with natural persons indicated as recipients. According to the GIFI, the transfers to natural persons were intended to create the appearance of a return on their "investment" and were intended to encourage them to make larger deposits. The GIFI was familiar with this pattern due to similar analytical cases conducted at the time.

In the course of the investigation initiated at the request of the GIFI (prior to the notification to the prosecutor's office, the GIFI blocked approx. EUR 60,000 on the bank accounts of the above-mentioned companies), the prosecutor's office established that the above-mentioned shareholder was the so-called unwitting "mule" (the companies were established using their data, but without their knowledge).

Twelve months after the GIFI took action, a letter was received from an authorised representative of a citizen of one of the EU countries – a sender of funds to the bank account of one of the above-mentioned companies. From the information and documents received, it appeared that this person had been convinced for more than a year that they had made a payment for a 12-month deposit offered by one of the Polish banks. The person became suspicious of the credibility of the offer received from the so-called broker only when the deposited funds were not returned to them after the expiry of the period. As a result of the GIFI's blockades, more than half of the funds deposited by the above-mentioned victim were recovered.

Information obtained by the GIFI indicates that, as part of the so-called broker scam, funds are defrauded not only under the guise of investments that are risky and often difficult for victims to understand (e.g. virtual currencies), but also under the guise of "safe" bank deposits.

Laundering of money derived from tax fraud using so-called courier brokers

The case concerned natural persons running sole proprietorships for the purpose of accepting cash-on-delivery parcels from others and sending them on their own behalf via known courier companies (obligated institutions). The GIFI identified and blocked the bank accounts of several such entities and sent notifications to the relevant prosecutors' offices.

The analysis of the statements provided by the above-mentioned obligated institutions showed that the consignments were addressed on the territory of Poland, as well as on the territory of other EU countries. In the case of only one entity (hereafter referred to as a courier broker), parcels with a C.O.D. value of more than PLN 201 million paid out to this customer were transferred via only one known courier company between 2020 and 2024⁴⁸ – recipients indicated more than 180.6 thousand different telephone numbers, with 335 different telephone numbers indicated by recipients of parcels with a C.O.D. value of more than PLN 100 thousand. More than 18,000 entities were recipients of the parcels. Funds from the courier broker's account were withdrawn in cash and transferred to undetermined persons. Similarly, in one case, a natural person marketing goods in Poland, after receiving payment for goods sold in their own online shop, to a bank account held in the name of their business, transferred these funds to their personal account and then withdrew significant amounts in cash, which they then

⁴⁸ Cash on delivery – charging for an order at the time of delivery of goods to the recipient.

transferred (via a well-known courier company) as payment for C.O.D parcels delivered on behalf of a courier broker.

The entities which were the recipients of the parcels sent by the courier broker were identified and the identification data of the entities to which the parcels were delivered was established. Analysis of the standard audit files for tax (JPK) submitted by them showed that the declared suppliers of the entities receiving parcels sent by the courier broker were:

- To a large extent, companies under investigation by prosecutors' offices across the country for suspected money laundering through their bank accounts,
- Companies that submit JPK files in which they mostly declare purchases from companies designated by the Head of the National Revenue Administration as entities at high risk of tax evasion,
- Entities whose activities are of interest to customs and tax control offices or are already subject to customs and tax controls,
- Companies established between 2022 and 2024, headquartered in virtual offices, with foreigners of Asian origin on their management boards, with share capital of PLN 5-10 thousand, declaring a monthly turnover in the range of PLN 1 million and amounts of output and input tax at similar levels,
- Companies that do not pay taxes to the State Treasury or, if they do, they pay inadequate amounts compared to their declared turnover,
- Entities that do not declare employment and payment of remuneration to employees at tax offices - no PIT-8C/11 declaration,
- Companies that have failed to disclose their material, technical, personnel and financial resources to make it plausible that they can actually carry out a business activity of trading in goods of the declared values.

An analysis of the purchase transactions declared in the submitted JPK files by the recipients of C.O.D parcels (sent by the courier broker), as well as an analysis of the transactions in the bank accounts of these entities, showed:

- A reverse supply chain – typically goods are sold from the manufacturer, through wholesalers, then to smaller distributors to the retailer. In contrast, in trading with the intent of VAT fraud, the goods are sold through a number of smaller entities that do not carry out actual business activities and are only used to issue fictitious invoices to larger distributors (as in the case of the courier broker's customers), who then introduce the goods to the final customer in the country via stationary or mail order sales,
- Purchasing from entities that do not carry out actual business activities, whose activities are/were the subject of the GIFI notifications submitted to prosecutors' offices across the country, as well as customs and tax controls,
- Withdrawal of almost all the profits from fiscal offences by a courier broker in cash in order to transfer them to alleged suppliers of goods, i.e. entities that do not actually carry out business activities, whose accounts have been blocked and whose activities are subject to customs and tax controls and investigations by prosecutors' offices across the country,

- The alleged suppliers of goods failed to disclose their material, technical, personnel and financial resources to make it plausible that they can actually carry out a business activity of trading in goods of the declared values. Thus, it is likely that these companies did not actually carry out business activities, but only issued invoices that did not document actual business events.

The courier broker is believed to have knowingly introduced goods of unknown origin into the Polish market by sending them in C.O.D parcels, for which the tax due had not been paid at previous marketing stages. On the other hand, the majority of recipients of the parcels knowingly sold these goods (through retail sales conducted by mail order companies or the Internet) on the Polish market, to consumers, obtaining benefits related to the commission of fiscal offences by themselves and the alleged suppliers of the goods. These funds were then transferred via courier companies to the sender of the parcels: the courier broker, and withdrawn in cash in order to hinder their detection, location, as well as seizure or forfeiture adjudication.

The GIFI points to the following practice: the listing of numerous fictitious suppliers is aimed, in addition to the undue VAT deduction, at avoiding the obligation to apply the regulation contained in Article 19 of the *Entrepreneurs' Law* to the purchase transactions.

In addition, the volume of cash deposits by both the courier broker and the recipients of the parcels, as well as the transactions declared by the recipients of the C.O.D parcels (including by the recipients of the parcels from the courier broker), testify to the involvement of these entities in the following practice: the recipients of the parcels from the courier broker purchased goods from unidentified suppliers who did not pay public liabilities, which they then sold via mail order companies and the Internet. The goods are of unknown origin, probably from China, and their value declared at customs may be understated. The goods are then delivered to the companies by persons who are not actually involved in the invoice trade (courier broker) and then sold for the actual market value of the product in question. At the same time, a number of entities allegedly brokering transactions for the sale of goods issue numerous fictitious invoices to justify the artificially created chain of suppliers. These are not entities genuinely carrying out business activities on their own responsibility and for their own account and are represented by persons acting as so-called "mules".

Payment to alleged suppliers is usually made in cash (transferred directly by the courier broker), with no disclosure of the persons actually collecting the receivables, who often do not have the authority to act on behalf of the declared supplier. As a consequence, part of the profits from fiscal offences committed ultimately goes to persons acting within an organised criminal group.

4.2. COUNTERACTING THE FINANCING OF TERRORISM

The main goal of the GIFI in the area of counteracting financing of terrorism is to cut terrorist organisations off their financing sources. The statutory tasks of the GIFI provide for obtaining, collecting, processing and analysing information in accordance with the statutory provisions and transferring it to the competent state authorities. Due to the variety of sources used to finance terrorism, the analysis covers both transactions reported to the GIFI as suspicious, as well as legal transactions carried out by entities in circumstances that give rise to suspecting them of being related to terrorist financing. Information used to initiate analyses comes mainly from cooperating units and the banking sector.

When performing its statutory tasks in the area of counteracting financing of terrorism in 2024, the GIFI initiated 16 analytical proceedings regarding transactions that could be related to financing of terrorism. 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 (FIU).

The proceedings initiated based on information from obligated institutions concerned usually transactions carried out by natural persons from 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 then the flows on personal bank accounts and money orders involving these persons. In cooperation with the Anti-Terrorist Centre of the Internal Security Agency⁴⁹, the GIFI analysed the connections with individuals or entities from countries with higher terrorist risk and identified their links with terrorist organisations. Verification of suspicions of terrorism financing led in some cases to their confirmation or detection of illegal commercial activities unrelated to terrorist financing, or on the contrary – to confirmation that certain transactions were carried out as part of legal financial activity conducted, e.g. due to family or business links, with entities based in higher risk countries.

Cooperation with foreign FIUs

Requests for information and spontaneous information related to financing of terrorism received from foreign FIUs, based on which analytical proceedings were initiated, usually related to transactions carried out by individuals residing in the territory of the Republic of Poland, who received funds from natural persons suspected of having links with terrorist groups or transferred funds to such natural persons. The GIFI verified such information, possibly extending its verification to include additional information, and then transferred it to the Internal Security Agency

Cooperation with the Internal Security Agency

In 2024, the GIFI received 21 letters from the Internal Security Agency regarding possible terrorism financing, including requests for information on individuals and entities suspected of financing of terrorism. The GIFI replied to all requests, forwarding the information received from institutions to the Internal Security Agency. In some cases, the information provided by the GIFI was supplemented with information received from foreign FIUs.

Additional information

As a result of analyses related to the aforementioned issues, the GIFI sent, pursuant to Article 106/106(1a) of the AML/CFT Act, a total of 34 notifications to the Internal Security Agency and one notification to the Prosecutor's Office regarding the possibility that a terrorist financing offence has been committed.

The GIFI is a member of the Interministerial Team for Terrorist Threats (ITTT) – an ancillary body of the Council of Ministers that is to ensure cooperation of the government administration bodies in preparing to prevent terrorist events, taking control over them through planned

⁴⁹ The Anti-Terrorist Centre of the Internal Security Agency is a coordination and analytical unit dedicated to counteracting and combating terrorism, among others, with respect to obtaining information on money laundering or fund transfers that may serve as evidence of terrorism financing.

activities and responding to them. The basic tasks of the Team include: monitoring terrorist threats as well as their analysis and assessment; presenting opinions and conclusions to the Council of Ministers; developing draft standards and procedures for responding to terrorist events, initiating, coordinating and monitoring activities undertaken by competent government administration bodies to prepare for preventing terrorist events, taking control over them through planned activities and responding to them; developing proposals aimed at improving the methods and forms of preventing terrorist events, preparing to take control over these events and responding where such events occur, as well as requesting competent authorities to undertake legislative work in this regard.

The key topics covered by the Team's work in 2024 included a multi-contextual assessment of the level of threat of a terrorist attack in Poland, taking into account the war in Ukraine, the situation on Poland's eastern border and the securing of the state border against illegal immigrants. The level of terrorist threat in Poland was also assessed in the context of revealed diversionary activities. Moreover, an important subject of the works of the above-mentioned Team was terrorist threats to the security of critical infrastructure facilities located in Poland and abroad, including key measures for the protection of critical infrastructure, such as ensuring its continuous operation, minimising the effects of possible disruptions, and quickly restoring its functions after failures. Another important aspect was discussing actions aimed at strengthening internal security and effectively countering terrorist threats with regard to counter-terrorism matters during the Polish Presidency of the Council of the European Union in the first half of 2025.

5. INSPECTIONS

5.1. INFORMATION FROM WHISTLEBLOWERS

Pursuant to Article 80 of the *AML/CFT Act*, the GIFI receives reports of actual or potential violations of the AML/CFT regulations from employees and former employees of obligated institutions or other individuals who perform or performed activities for obligated institutions on a basis other than an employment relationship. Therefore, in order to fulfil this obligation, the GIFI has enabled submitting the aforementioned reports in electronic form to the email address: sygnalisci.GIIF@mf.gov.pl, or sending them in paper form to the correspondence address indicated by the GIFI.

Based on the information received by the GIFI in 2024, 52 cases were entered in the whistleblowing register. Irregularities identified in whistleblowers' reports concerned, among others, suspected fiscal offences, failure to perform obligations under the *AML/CFT Act* by obligated institutions, or illegal business activities. Some of the reports received by the GIFI were transferred to the competent authorities so that they could perform their statutory tasks.

Moreover, in accordance with Article 53a of the *AML/CFT Act*, the GIFI also receives reports regarding retaliation against employees and persons performing activities for obligated institutions. To this end, the GIFI has enabled submitting reports in electronic form to the email address (GIIF.53a@mf.gov.pl) or in paper form to the correspondence address indicated by the GIFI. Although various messages were sent to the above email address, none of them met the statutory reporting requirement, and thus no case was registered.

5.2 INSPECTIONS PERFORMED BY THE GIFI

Pursuant to the provisions of the *AML/CFT Act*, in 2023, the GIFI carried out nine inspections in the following obligated institutions (according to the date of the post-inspection statement, i.e. post-inspection statements in 2024):

- one cooperative savings and credit union;
- six virtual asset service providers;
- one postal operator;
- one entity carrying out betting activities;

The inspections revealed irregularities in the fulfilment of the obligations under the *AML/CFT Act* by the inspected obligated institutions. The inspections revealed a total of 179 irregularities related to formal and substantive shortcomings were found, mainly regarding the improper use of customer due diligence measures. The irregularities identified included:

1. Formal shortcomings:

- failure to implement the assessment of the risk of money laundering and financing of terrorism referred to in Article 27 of the *AML/CFT Act* or to adapt it to the provisions thereof;

- failure to implement internal procedures regarding AML/CFT regulations referred to in Article 50 and Article 53 of the *AML/CFT Act* or to adapt them to the provisions thereof.

2. Substantive shortcomings:

- failure to appoint the relevant persons as defined in the *AML/CFT Act*;
- failure to ensure the participation of persons performing AML/CFT duties in training programmes on the implementation of these duties;
- failure to carry out or improperly carrying out the analysis and risk assessment related to business relationships or to occasional transactions, as referred to in Art. 33(2)–(3) of the *AML/CFT Act*;
- failure to apply customer due diligence measures, linked to risk assessment;
- violation of the obligation to provide the GIFI with information pursuant to Article 76 of the *AML/CFT Act* (including as part of so-called "quarterly reporting") and Article 72 of the *AML/CFT Act*;
- failure to comply with the obligation to notify the GIFI, pursuant to Article 74 of the *AML/CFT Act* or Article 86 of the *AML/CFT Act*.

As for the identified violations, the GIFI issued post-inspection recommendations to the obligated institutions concerned so that they fulfil their obligations under the *AML/CFT Act*.

They were recommended, among others, to:

- adapt/implement the procedures in accordance with Article 50 and Article 53 of the *AML/CFT Act* and to fulfil the obligation referred to in Article 27(1-3) of the *AML/CFT Act*;
- formally appoint the person(s) specified in the *AML/CFT Act*;
- ensure the participation of persons performing duties related to counteracting money laundering and financing of terrorism in training programmes;
- fulfil the obligation to identify the ML/TF risk related to a business relationship or an occasional transaction, and to assess the risk level in accordance with Article 33(2)-(3) of the *AML/CFT Act*;
- take action to reliably apply customer due diligence measures;
- properly fulfil the obligation to submit information to the GIFI, as referred to in Article 72 of the *AML/CFT Act* (including submission of all information specified in the provision and submission of information in a timely manner) and as referred to in Article 76 of the *AML/CFT Act* (including with regard to so-called "quarterly reporting");
- notify the GIFI, in accordance with Article 74 or Article 86 of the *AML/CFT Act*, while making sure to include all mandatory elements set out in Article 74(3) of the Act and the practical information provided by the GIFI;

In 2024, the GIFI sent 3 notifications to the prosecutor's office regarding employees of obligated institutions indicating a reasonable suspicion of committing an offence under Article 156(1)(1) of the *AML/CFT Act*.

5.3. INSPECTIONS CARRIED OUT BY SUPERVISORY INSTITUTIONS

Pursuant to the provisions of Article 131(5)(3) of the AML/CFT Act, supervisory institutions provide the GIFI with information on the findings of inspections carried out. According to the data held by the GIFI, a total of **492 inspections** were carried out in 2024, of which:

- the National Bank of Poland carried out **368** inspections:⁵⁰
- the Polish Financial Supervision Authority carried out **17** inspections,
- Customs and Tax Control Offices carried out **22** inspections,
- ministers, voivodeship governors and poviats governors carried out **18** inspections,
- the National Cooperative Savings and Credit Union carried out **6** inspections,
- Presidents of Courts of Appeal carried out **61** on-site visits.

5.4. ADMINISTRATIVE PROCEEDINGS REGARDING IMPOSITION OF ADMINISTRATIVE SANCTIONS

Pursuant to the provisions of the *AML/CFT Act*, proceedings concerning imposition of administrative sanctions on obligated institutions for irregularities in the performance of the obligations referred to in Article 147, Article 148 and Article 149 of the *AML/CFT Act*, shall be conducted in accordance with the provisions of the Code of Administrative Procedure. Imposition of administrative sanctions is part of the GIFI competence.

In determining the type of administrative sanction and its amount, the GIFI shall take into account the circumstances listed in Article 150(4) of the *AML/CFT Act*, including the gravity and duration of the breach, the extent of the obligated institution's responsibility and its financial capacity. The GIFI conducts administrative proceedings following its own inspections and inspections carried out by heads of customs and tax control offices, presidents of courts of appeal, the National Cooperative Savings and Credit Union, ministers, governors of provinces (voivodes) and governors of districts. The number of administrative proceedings conducted by the GIFI is also closely linked to the number of inspections it conducts.

In 2024, GIFI initiated 17 administrative proceedings. Six of them were initiated in connection with irregularities identified as a result of inspections carried out by the GIFI, while the remaining eleven were launched as a result of inspections carried out by other authorities. In

⁵⁰ The above figure refers to currency exchange office operators who were inspected. A total of 602 currency exchange offices were inspected as part of these activities. The inspections revealed AML/CFT irregularities in 119 exchange offices, operated by 76 businesses. Irregularities in compliance with obligation under the *AML/CFT Act* related to such things as failure to appoint managers or employees responsible for ensuring the obligated institution's compliance with the *AML/CFT Act*; lack of or failure to update the ML/TF risk assessment; risk assessment inadequate for the business; failure to apply or document customer due diligence measures; failure to keep the results of ongoing analysis of transactions carried out; lack of internal procedure of the obligated institution; lack of or insufficient training programmes for the business; failure to provide the GIFI with information on transactions above 15,000 euros; failure to submit information to the GIFI on time or the incompleteness of such information. In 2024, 33 entrepreneurs were sanctioned due to non-compliance with obligations under the *AML/CFT Act*. There were 31 decisions to impose a fine and 2 decisions to require the publication of information in the Public Information Bulletin. The total value of fines imposed for decisions issued in 2024 was PLN 441,500.00.

2024, the GIFI completed 16 proceedings with administrative decisions regarding the imposition of administrative sanctions. In 2024, 9 appeals against GIFI decisions were submitted to the Minister of Finance. In the same period, the Minister of Finance issued a total of 8 administrative decisions.

In 2024, two complaints against the decisions of the Minister of Finance were submitted to the Voivodeship Administrative Court. The Voivodeship Administrative Court issued three decisions in this respect, dismissing all complaints against the Minister's decisions. In 2024, two cassation complaints were filed by the parties against Voivodeship Administrative Court decisions related to decisions of the Minister of Finance. In 2024, the Supreme Administrative Court settled one case, dismissing the cassation complaint of a party.

6. NATIONAL COOPERATION

6.1 EXCHANGE OF INFORMATION WITH DOMESTIC ENTITIES

Competent authorities — primarily the prosecutor's office and other law enforcement agencies — used the data held by the GIFI. Information collected in the manner and scope specified in the *AML/CFT Act* was made available by the GIFI at the request of courts and prosecutors for the purpose of criminal proceedings in accordance with Article 104 of the *AML/CFT Act*. Information on transactions was also transferred by the GIFI on request to the services subordinated to and supervised by the minister competent for the interior: the Police and the Border Guard, as well as the Heads of the Internal Security Agency, the Military Counter-Intelligence Service, the Central Anti-Corruption Bureau (hereinafter referred to as CBA) under Article 105(1) of the *AML/CFT Act*. Other bodies authorised to obtain transaction information included the Head of the National Revenue Administration, directors of revenue administration regional offices, heads of customs and tax control offices, and other bodies in accordance with Article 105(3) of the *AML/CFT Act*.

Since 13 July 2018, the organisational units of prosecutors' offices have been obliged to provide information on issued decisions to block a bank account or suspend a transaction, initiate proceedings, present charges and bring an indictment, in cases related to a money laundering or terrorism financing offence, under Article 81 of the *AML/CFT Act*. The other law enforcement agencies authorised to conduct criminal proceedings (as well as other cooperating units) submitted notifications of a suspected money laundering or terrorism financing offence under Article 83(1) and (2) of the *AML/CFT Act*.

The quantitative data analysis concerning the exchange of information with domestic entities shows stabilised cooperation with the GIFI. The number of requests addressed to the GIFI by organisational units of the prosecutor's office increased, as well as the number of information provided by organisational units of the prosecutor's office on the basis of Article 81 of the *AML/CFT Act* increased once again.

6.1.1. COOPERATION WITH ORGANISATIONAL UNITS OF THE PROSECUTOR'S OFFICE AND COURTS

Pursuant to Article 104 of the *AML/CFT Act*, in 2024, the GIFI received from organisational units of the prosecutor's office 681 requests for information concerning at least 2,961 entities (in 2023, the GIFI received 593 requests for information concerning 3,402 entities). It should also be emphasized that the requests submitted in 2024 concerned at least 1,650 bank accounts.

In recent years, the cooperation with the prosecutor's offices has been more effective, as confirmed by the still large number of requests for information submitted to the GIFI by the organisational units of prosecutor's office.⁵¹ In 2024, just like in 2021–2023, there was an

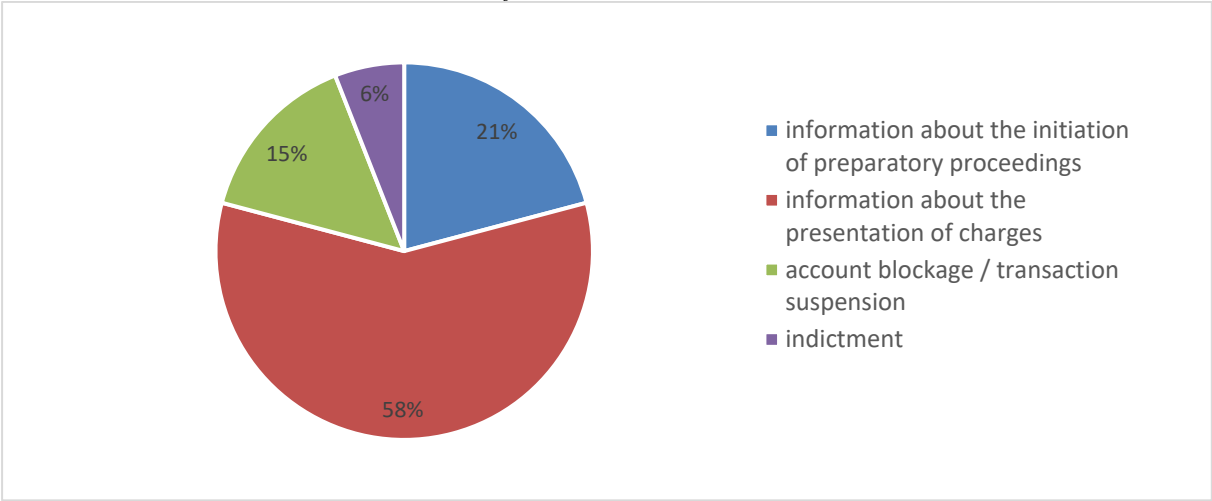
⁵¹ Starting from 2014, organisational units of prosecutors' offices submitted over 500 requests for information each year, which is a significant increase compared to the preceding years (in 2013, 400 requests were recorded).

increase in the number of such requests, which referred to assets and were largely aimed at identifying assets. Furthermore, with the use of requests for information and the information thus obtained, the organisational units of the prosecutor’s office were able to present charges to suspects to a greater extent, in particular under Article 299 of the *Penal Code*.

In 2024, the GIFI also received 14 requests for information from the courts, which concerned 12 entities. By comparison, there were 12 such requests to the GIFI from the courts in 2023, with respect to nine entities.

In 2024, the GIFI received 463 pieces of information under Article 81 of the *AML/CFT Act* from organisational units of prosecutor’s office (the prosecutor notifies the GIFI of issuing a decision to block a bank account or suspend a transaction, initiation of proceedings, presenting charges and bringing an indictment in cases related to a money laundering or terrorist financing offence), which means an increase compared to 2023, when this figure was 383.

Chart 12. Breakdown of information received from organisational units of prosecutor’s office under Article 81 of the *AML/CFT Act* in 2024



In 2024, prosecutors typically transferred information on initiation of proceedings regarding a suspected offence referred to in Article 299 of the *Penal Code* (91 pieces of information) or presenting charges under this provision (254 pieces of information). In 26 cases, the information concerned bringing an indictment. In the remaining cases (65), organisational units of prosecutor’s office requested the GIFI to consider undertaking its statutory activities to block bank accounts or suspend transactions.

Based on the information submitted by the competent authorities under Article 81 of the *AML/CFT Act*, the GIFI carried out its statutory activities to deny criminals access to assets, thus preventing them from legalising proceeds from prohibited acts. As a result of such cooperation, the GIFI sent to the competent organisational units of prosecutors’ offices — based on the information received — notifications of a suspected offence referred to in Article 299 of the *Penal Code*.

In 2024, just like in previous years, organisational units of prosecutor’s office also happened to submit in a single letter information under Article 81 of the *AML/CFT Act*, simultaneously requesting information under Article 104(1) of the *AML/CFT Act*, enabling a more effective and efficient exchange of information. The GIFI recorded 49 such cases.

It should be emphasised that when acting in accordance with Article 81(4) of the *AML/CFT Act*, the GIFI immediately notifies the prosecutor of being in possession of information related to the information submitted under Article 81(1) of the *AML/CFT Act*. In 2024, information provided by organisational units of prosecutor's office was frequently related to information held by the GIFI. In such situations, whenever a positive response from the GIFI was obtained, the information held by the GIFI was requested, which in many cases had an impact on further procedural activities carried out by organisational units of prosecutor's office, e.g. in the form of extending the range of charges presented to suspects.

In 2024, secure electronic information exchange channels were used to cooperate with organisational units of prosecutor's office. These secure electronic information exchange channels were also used by the GIFI to obtain information from obligated institutions from which information was received on transactions covered by the provisions of the *AML/CFT Act* for the purposes of cooperation between the GIFI and organisational units of prosecutor's office. It was largely due to the subject of the requests, that concerned a large number of entities or a large number of accounts. Providing this data in an electronic version, and even more in an editable form, greatly accelerated the process of handling the requests. Furthermore, such cases also related to accelerating the response by the GIFI, due to urgent procedural activities carried out by organisational units of prosecutor's office.

Cooperation with organisational units of the public prosecutor's office, involving the participation of representatives of the Department of Financial Information in initiatives aimed at exchanging experience in AML/CFT, continued in 2024. This made it possible to disseminate good practices aimed at ensuring a more effective interaction between the GIFI and representatives of organisational units of the public prosecutor's office.

6.1.2. COOPERATION WITH THE NATIONAL REVENUE ADMINISTRATION BODIES

In 2024, the GIFI received 102 requests from the heads of customs and tax control offices regarding 245 entities. This means a decrease in the number of submitted requests compared to 2023, when the GIFI received 119 requests concerning 283 entities.

As part of this cooperation, increased effectiveness of cooperation with the National Revenue Administration bodies could still be observed. In 2024, the exchange of request-related correspondence repeatedly resulted in the commencement of further cooperation between the authorities under Article 83 of the *AML/CFT Act*. As a result of this cooperation, the GIFI sent to the competent organisational units of prosecutor's office — based on the information received from the National Revenue Administration bodies — notifications of a suspected offence referred to in Article 299 of the *Penal Code*. The statutory activities undertaken by the GIFI were also intended to deny criminals access to assets, and thus prevent them from legalising proceeds from prohibited acts, in this case particularly from fiscal offences.

In 2024, the GIFI also received 40 requests for information from directors of revenue administration regional offices regarding 48 entities, compared to 101 requests received in 2023 with respect to 132 entities.

In 2024, representatives of the management of the Department of Financial Information participated in quarterly meetings with the management of the National Revenue

Administration, where they had the opportunity to provide information on good practices aimed at ensuring more effective cooperation between the GIFI and the Administration's organisational units.

6.1.3. COOPERATION WITH BODIES SUBORDINATED TO THE MINISTER OF THE INTERIOR

In 2024, pursuant to Article 105(1) of the *AML/CFT Act*, the GIFI received 119 requests for information from the Police organisational units, which concerned 857 entities (compared to 141 request concerning 908 entities received in 2023), whose significant part was submitted by authorised individuals representing the Office for Combating Economic Crime of the Police Headquarters, the Central Investigation Bureau of the Police and the Central Cybercrime Bureau. As in previous years, cooperation related to the processing of requests for representatives of the Police bodies was smooth and effective.

Moreover, in 2024, the GIFI replied to 23 requests concerning 261 entities, submitted by authorised representatives of the Headquarters of the Border Guard, which represents an increase in the number of requests compared to 2023, when the GIFI received 35 requests concerning 264 entities.

Units supervised by and subordinate to the minister competent for the interior also fulfilled the obligations specified in Article 83(1) of the *AML/CFT Act*, which significantly extended cooperation in counteracting the offence specified in Article 299 of the *Penal Code*. In 2024, the GIFI received 53 such pieces of information from the Police organisational units, concerning 269 entities.

Based on the information received, the GIFI was able to more effectively fulfil its statutory obligations, also by blocking accounts. The activities undertaken with respect to analyses conducted by the GIFI enabled more effective cooperation already at the stage of operational and reconnaissance work of services subordinate to and supervised by the minister competent for the interior, including, in particular, in identifying assets at the initial stage of operational and reconnaissance activities, as well as later, at the investigation stage.

In June 2024, a representative of the Department of Financial Information took part in the sixth edition of the ICT Crime XXI conference in Gdynia, which focused on issues related to combating cybercrime. The event was co-organised by the Central Cybercrime Bureau.

In addition, in 2024 a representative Department of the Financial Information took part in another edition of the tax course implemented for police officers by the Police Academy in Szczytno, as well as in the next edition of the AML course implemented for police officers by the Police Academy in Piła.

6.1.4. COOPERATION WITH STATE SECURITY SERVICES

In 2024, the GIFI received 15 requests for information held by it from the Military Counter-Intelligence Service. The requests concerned 33 entities. To compare, in 2023, the GIFI received 21 requests concerning 33 entities

In 2024, as part of national cooperation, the GIFI received from the Head of the Internal Security Agency — pursuant to Article 105(1) of the *AML/CFT Act* — 56 (compared to 35 in 2023) requests for providing by the GIFI information about persons/entities suspected of committing financing of terrorism offences, offences affecting the economic foundations of the state, and offences involving the production of and trade in goods, technologies and services of strategic importance for state security. In 2024, the GIFI also received from the Internal Security Agency one (in 2023, also one) piece of information on a suspected money laundering or financing of terrorism offence pursuant to Article 83(1) of the *AML/CFT Act*.

6.1.5. COOPERATION WITH THE CENTRAL ANTI-CORRUPTION BUREAU

In 2024, under Article 105(1) of the *AML/CFT Act*, the GIFI received from the Central Anti-Corruption Bureau 6 requests for information regarding at least 44 entities, and 7 notifications concerning 28 entities, provided pursuant to Article 83(1) of the *AML/CFT Act*.

Given the 17 requests regarding 70 entities received in 2023, the GIFI's cooperation with the Central Anti-Corruption Bureau diminished in 2024.

6.1.6. COOPERATION WITH OTHER AUTHORITIES

In 2024, the Minister of Finance sent to the General Inspector of Financial Information 30 requests pursuant to Article 11(2) of the *Gambling Act of 19 November 2009*. The replies to the requests concerned a total of 133 entities.

In 2024, the GIFI received 17 requests for information held by it from the Chair of the Polish Financial Supervision Authority. The requests concerned 435 entities.

In 2024, the GIFI also received 23 requests for information from the Military Police, that concerned 64 entities. To compare, in 2023, the Military Police submitted 55 requests concerning 112 entities.

6.1.7. COOPERATION WITH THE NATIONAL CENTRE FOR CRIMINAL INFORMATION

In 2024, the GIFI cooperated with the Head of the National Centre for Criminal Information (KCIK). The GIFI sent 1,148 inquiries, including 766 requests to supplement information as well as 770 requests to obligated entities.

The KCIK also submitted inquiries to the GIFI. In 2024, these concerned 2286 entities. After checking its databases, the GIFI replied in 463 cases that the subject indicated in the inquiry was identified in the analytical proceedings carried out by the GIFI. Inquiries from the National Centre for Criminal Information are sent to the GIFI electronically, in an agreed format, which enables a partial automation of the generation and provision of reports. In 2024, the aforementioned inquiries concerning 2,286 entities were submitted in the form of 125 electronic files, directly to the GIFI's IT system. Generation and provision of a response (to be directly downloaded from the secure website of the GIFI's ICT system) usually takes a few days.

6.2 Feedback

The prosecutor's office may provide feedback to the notifying body at various stages of ongoing criminal proceedings. The information provided by prosecutors may take various forms and concern various aspects of criminal proceedings. The prosecutor's decision may include an assessment of the collected evidence and present the procedural actions taken. The provision of Article 107 of the *AML/CFT Act* is a special one under which (and also pursuant to the relevant provisions of the Code of Criminal Procedure) prosecutors are obliged to provide feedback on actions taken in connection with notifications of a suspected money laundering or financing of terrorism offence received from the GIFI (this applies to information on: issuance of a decision to block an account or suspend a transaction; suspension of proceedings; resumption of suspended proceedings; issuance of a decision to present a charge of committing an offence). The data presented below concern the volume of all types of feedback received by the GIFI from prosecutors (in the form of pleadings) prepared in the course of preparatory proceedings. The information concerned is related to analytical proceedings in which the GIFI sent notifications of a suspected offence to the prosecutor's office in 2024.

Chart 13. Breakdown of feedback received from prosecutors in 2020-2024, related to analytical proceedings in which the GIFI sent notifications of a suspected offence to the prosecutor's office, by information type⁵²

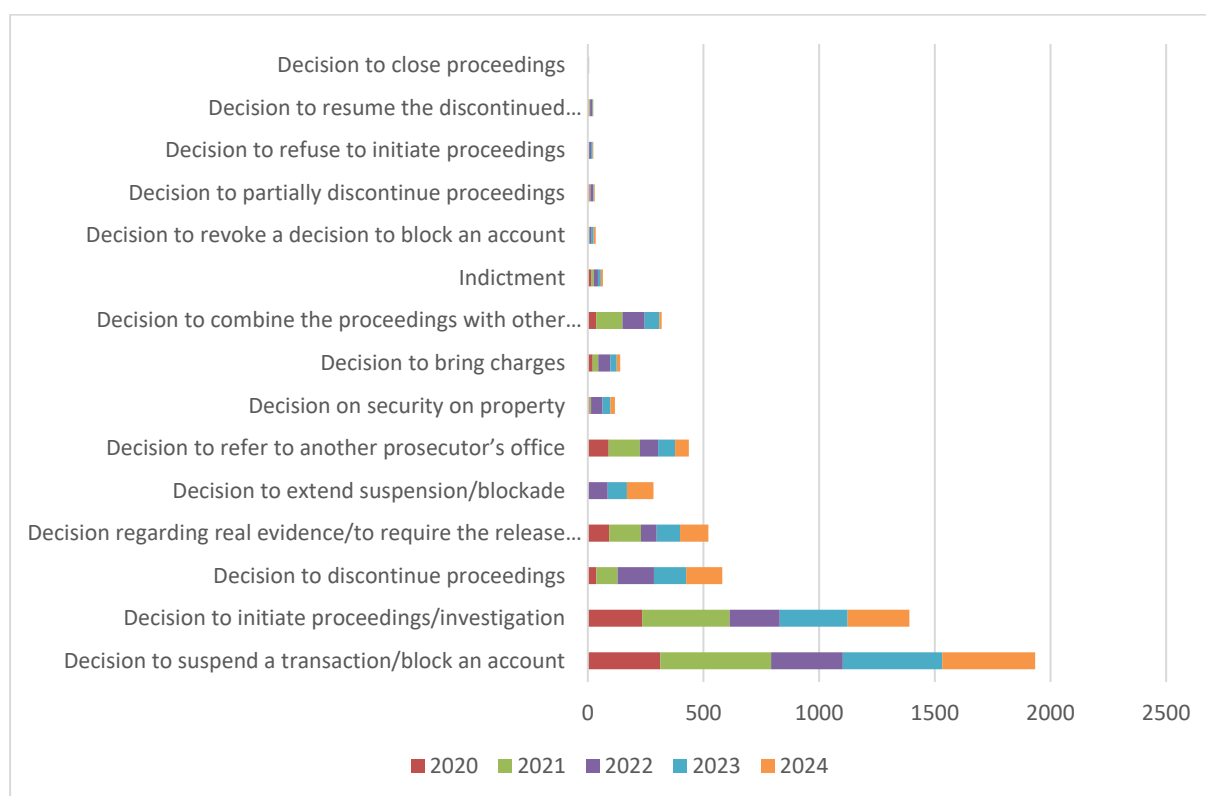


Table 5. Breakdown of feedback from prosecutors⁵³

Breakdown of feedback from prosecutors (Chart 13)	2020	2021	2022	2023	2024
---	------	------	------	------	------

⁵² According to information recorded in the GIFI's IT system as of 20 February 2025.

⁵³ Besides the above information, the GIFI also received information about other decisions issued by prosecutors, in particular information on decisions to suspend criminal proceedings or to resume suspended proceedings.

Decision to suspend a transaction/block an account	313	479	310	430	402
Decision to initiate proceedings/investigation	235	378	217	293	267
Decision to discontinue proceedings	37	92	157	139	156
Decision regarding real evidence/to require the release of specific item(s)	92	138	68	101	122
Decision to extend suspension/blockade	0	0	86	83	115
Decision to refer to another prosecutor's office	90	135	79	73	60
Decision on security on property	8	6	50	34	19
Decision to bring charges	21	24	52	28	15
Decision to combine the proceedings with other proceedings/investigation	36	114	96	63	10
Indictment	14	12	18	12	9
Decision to revoke a decision to block an account	2	5	7	11	9
Decision to partially discontinue proceedings	8	3	12	3	4
Decision to refuse to initiate proceedings	2	4	8	7	3
Decision to resume the discontinued proceedings/investigation	6	4	8	4	2
Decision to close proceedings	1	1	2	1	1

6.2.1 NATIONAL REVENUE ADMINISTRATION BODIES

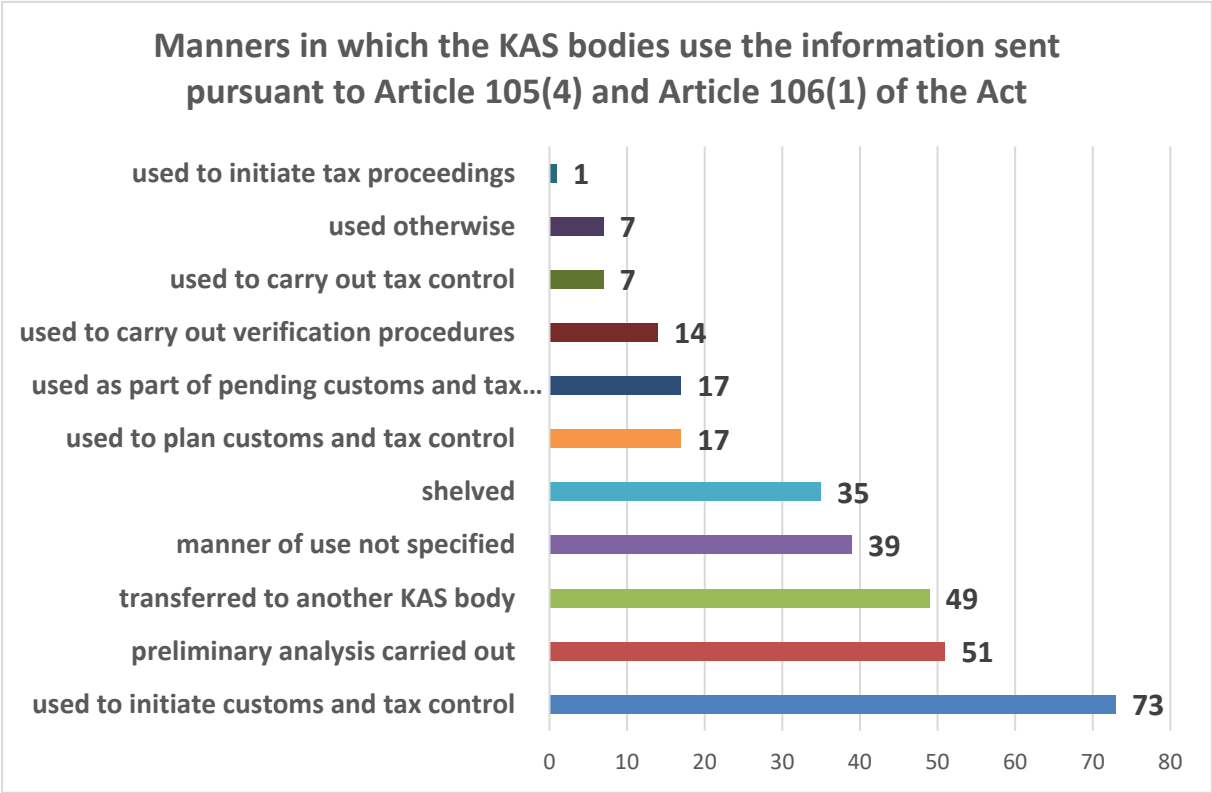
The National Revenue Administration is a specialist government administration body that performs tasks regarding income from taxes, customs duties, fees and non-tax budget receivables, protection of the interests of the State Treasury and protection of the customs territory of the European Union. It also provides services and support to taxpayers and tax remitters in the proper performance of their tax obligations, as well as to economic operators in the proper performance of their customs obligations. The KAS includes the Customs and Tax Service — a uniform and uniformed formation made up of officers. The authorised KAS bodies receive information from the GIFl that is relevant to their statutory tasks. The KAS usually used the information provided by the GIFl in its analyses and checks to identify threats in the areas subject to its supervision, in particular in terms of the performance of the obligations related to public levies. In the Polish legal system, violations of prohibitions and orders under financial law falling within the responsibilities of the Minister of Finance, i.e. tax law, customs law, foreign exchange law and gambling law, are penalised under the *Act of 10 September 1999 — Fiscal Penal Code* (consolidated texts: Journal of Laws of 2024, item 628) and under the *Act of 6 June 1997 — Penal Code* (consolidated text: Dz.U. /Journal of Laws/ of 2024, item 17, as amended). The information requested by the KAS bodies from the GIFl was, among other things, to confirm or exclude identified mechanisms of fiscal fraud and to indicate other entities suspected of involvement in fiscal crimes and offences. The information received was used in determining whether a customs and tax control or a tax control as well as preliminary proceedings should be initiated in cases regarding a suspected fiscal offence, as well as in the course of such controls and proceedings. The purpose of these activities is to ensure the proper enforcement of taxes and to secure the State Treasury levies.

On the other hand, the information submitted to the KAS bodies by the GIFI on its own initiative (under Article 106(1) of the *AML/CFT Act*) was analysed for its possible relation with suspected fiscal offences.

The GIFI received information from individual KAS bodies pursuant to Article 14(5) of the *AML/CFT Act*, which showed that in 2024, based on information received from the GIFI (both under 105(4) and Article 106(1) of the *AML/CFT Act*):

- at least 73 pieces of information were used to initiate tax and customs inspections;
- a preliminary analysis is being conducted for at least 51 pieces of information;
- 49 pieces of information were forwarded to another KAS body;
- for at least 35 pieces of information, copies were retained *on file*;
- at least 17 pieces of information served as a basis for planning tax inspections;
- at least 17 pieces of information were used in the course of ongoing tax inspections;
- at least 14 pieces of information were used in the course of verification procedures;
- at least 7 pieces of information were used to carry out tax inspection;
- at least one piece of information was used to initiate tax proceedings;
- at least 7 pieces of information were used in other ways. According to the information provided by the KAS bodies, this category refers to those cases where the GIFI information was used to delete an entity from the register, to apply for deletion from the National Court Register, to withdraw from proceedings, to initiate an audit or proceedings with regard to another entity, etc.

Chart 14. Breakdown of information received by the KAS bodies from the GIFI by the method of its use



6.2.2 THE POLICE

According to the information received from the Police Commander in Chief, in 2024, the Criminal Bureau of the Police Headquarters received 97 pieces of information from the GIFI under Article 106(1) of the *AML/CFT Act*. Each piece of information received by the Criminal Bureau of the Police Headquarters was transferred to locally and materially competent organisational units of the Police for official activities to be taken, including:

- data obtained based on 5 pieces of information was transferred to evidence collected as part of ongoing preparatory proceedings;
- 110 pieces of information obtained from the GIFI were verified as part of operational and reconnaissance activities; in 5 cases, the performed activities did not confirm the information received.

In 2024, pursuant to Article 105(1)(1) of the *AML/CFT Act* (at the request of the Police Commander in Chief), the GIFI provided information in 20 cases in connection with pending operational cases. The information provided by the GIFI is still being analysed and supplemented with self-made findings, and it is used in ongoing operational and reconnaissance activities carried out by the Police organisational units. In 2024, the Police also provided the GIFI with a total of 15 pieces of information pursuant to Article 83(1) of the *AML/CFT Act*.

According to the information provided by the Central Investigation Bureau of the Police pursuant to Article 14(5) of the *AML/CFT Act*, in 2024, this Bureau submitted 41 requests for

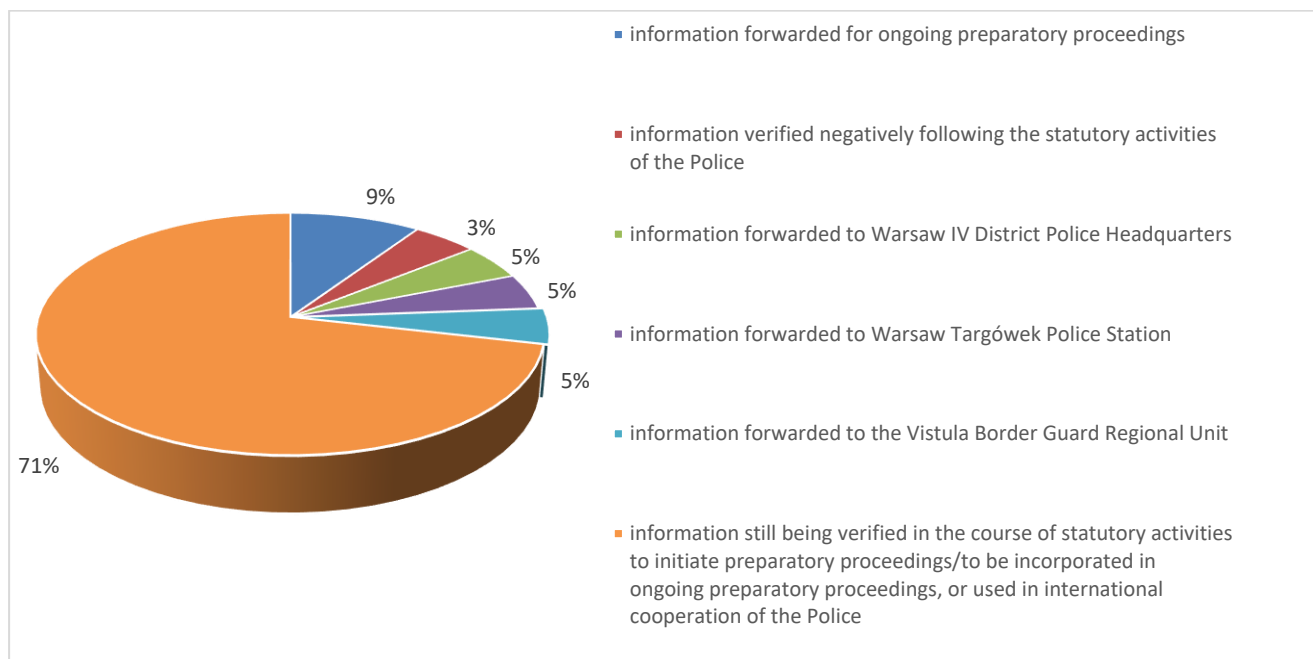
information to the GIFI.⁵⁴ Following its analysis, the received information was used in operational activities, including:

- in seven cases, the information was forwarded to ongoing preparatory proceedings;
- in three cases, the information was used as part of international cooperation of the Police;
- in one case, the obtained information was verified negatively — based on the decision of the prosecutor supervising the preparatory proceedings;
- in five cases, the response received from the GIFI indicated the lack of information on transactions or bank accounts of the individuals or business entities covered by the requests;
- in the case of eighteen applications, the obtained information is still being verified by the Central Investigation Bureau of the Police as part of its statutory activities. As part of these activities, among others, a criminal analysis is being carried out and the documentation is being prepared to be transferred to an organisational unit of the prosecutor's office to initiate preparatory proceedings/to be incorporated in ongoing preparatory proceedings;
- seven cases are pending a response from the GIFI (as of 28 January 2025);

The Central Investigation Bureau of the Police reported that it initiated 17 preparatory proceedings under Article 299 of the *Penal Code* in 2024. Moreover, the Central Investigation Bureau of the Police did not record any cases of initiation and termination of preparatory proceedings under Article 165a of the *Penal Code*. According to the information in question, in the proceedings conducted by the Central Investigation Bureau of the Police, 732 suspects were charged with a total of 970 offences under Article 299 of the *Penal Code*.

⁵⁴ These included requests for information on 300 individuals, 164 business entities and 29 bank accounts.

Chart 15. Breakdown of notifications received by the Central Investigation Bureau of the Police from the GIFI by the method of their use



In 2024, the Central Investigation Bureau of the Police received from the GIFI a total of 21 pieces of information under Article 106(1) and (1a) of the *AML/CFT Act*. The information was used as follows:

- 2 pieces of information were forwarded to ongoing preparatory proceedings;
- 1 piece of information, following the relevant statutory activities taken by the Police, was verified negatively;
- 1 piece of information was forwarded to Warsaw IV District Police Headquarters;
- 1 piece of information was forwarded to Warsaw Targówek Police Station;
- 1 piece of information was forwarded to the Vistula Border Guard Regional Unit;
- 15 pieces of information are still being verified in the course of statutory activities, as part of which, among others, a criminal analysis is being carried out and the documentation is being prepared to be transferred to an organisational unit of the prosecutor's office to initiate preparatory proceedings/to be incorporated in ongoing preparatory proceedings, or its use in international cooperation of the Police is being considered.

Information received from the Central Cybercrime Bureau Commander shows that in 2024, pursuant to Article 105(1)(13) of the *AML/CFT Act* (at the request of the Central Cybercrime Bureau Commander), the GIFI provided information in fifteen cases in connection with operational cases and in one concerning preparatory proceedings. Two of the aforementioned pieces of information were forwarded to the public prosecutor's office for inclusion in the ongoing investigation, and a further two were sent to the public prosecutor's office with a request to initiate proceedings. In addition, one piece of information is being analysed for inclusion in ongoing proceedings.

Acting under Article 106(1) of the *AML/CFT Act*, the GIFI provided the Central Cybercrime Bureau Commander with six pieces of information in 2024. Each time, the material was forwarded to the Central Cybercrime Bureau's locally and materially competent units to take official action. The information obtained by the Central Cybercrime Bureau was used as follows:

- one piece of information was verified through operational and reconnaissance activities, which did not confirm it;
- one piece of information was forwarded to the Central Investigation Bureau of the Police;
- four pieces of information were used in ongoing operational and reconnaissance activities as part of which the information is still being processed, analysed, supplemented and correlated.

The Central Cybercrime Bureau also reported that it opened fourteen preparatory proceedings for offences under Article 299(1) of the Penal Code and six proceedings for those under Article 299(5) thereof in 2024. In the same period, fourteen proceedings were completed for offences under Article 299(1) of the Penal Code and seven for those under Article 299(5) thereof. All these proceedings concerned money laundering. Moreover, in 2024, the Central Cybercrime Bureau forwarded a total of six notifications of suspected money laundering to the GIFI under Article 83(1) of the *AML/CFT Act*.

6.2.3. OTHER AUTHORITIES

According to data received from the Internal Security Agency pursuant to Article 14(5) of the *AML/CFT Act*, in 2024, the Agency received from the GIFI at least 76 letters of various levels of classification, 57 of which were responses to the Agency's requests for information, executed under Article 105 of the aforementioned Act. Additionally, the Internal Security Agency reported that it received at least 19 letters constituting notifications/information in 2024, sent on the GIFI's own initiative. Based on the information provided by the GIFI, actions were taken within the framework of detailed operational procedures implemented under Article 5(1)(2) of the *Act on the Internal Security Agency and the Intelligence Agency* (recognition, prevention and detection of such offences as espionage; terrorism; offences affecting the economic foundations of the state; corruption; offences involving the production of and trade in goods, technologies and services of strategic importance for state security; illegal production, possession and trade in weapons, ammunition and explosives; crimes related to WMDs and narcotic drugs and psychotropic substances; crimes in international trade; crimes against the administration of justice). The knowledge based on GIFI information was used in the ongoing work of the relevant divisions of the Agency. In addition, the Internal Security Agency sent 3 letters to the GIFI in 2024 pursuant to Article 83(1) of the *AML/CFT Act*.

The Central Anti-Corruption Bureau indicated that it had received a total of 11 pieces of information from the GIFI under the *AML/CFT Act* in 2024. Of the above, 5 were sent by the GIFI on its own initiative under Article 106 of the *AML/CFT Act*. The Central Anti-Corruption Bureau's official activities used the notifications received in 7 types of activities:

- 1 piece of information was used in operational and reconnaissance activities;
- 2 pieces of information were used in investigation activities;

- 3 pieces of information were forwarded to another organisational unit;
- 1 piece of information was forwarded to another body;
- furthermore, no action was taken for 1 piece of information.

The Central Anti-Corruption Bureau also stated that it had received 6 information requests under Article 105 of the *AML/CFT Act* in response to information requests submitted to the GIFI during 2024.

The Border Guard Headquarters informed that in 2024, it received from the GIFI a total of 28 pieces of information. Of these, 21 were made available by the GIFI at the written and substantiated request of the Border Guard, while 7 were provided by the GIFI in connection with the GIFI's suspicion of an offence other than money laundering or financing of terrorism to enable action to be taken in accordance with the statutory tasks of the Border Guard.

The Bureau of Internal Affairs of the Border Guard reported that no requests for information were made to the GIFI under Article 105 of the *AML/CFT Act* in 2024.

By contrast, it is known from information provided by the Military Counter-Intelligence Service that the Service made fourteen requests for information to the GIFI in 2024. No activities other than internal analytical and technical procedures were undertaken by the Military Counter-Intelligence Service based on information received from the GIFI. The Military Counter-Intelligence Service did not transfer the information obtained from the GIFI to other authorities or public administration bodies, nor did it use this information to carry out other “further activities” within the meaning of Article 14(2)(11) of the *AML/CFT Act*.

The data for 2024 obtained from the Military Police Headquarters indicate that in 2024, the Military Police obtained from the GIFI, in response to 31 requests it submitted, 31 pieces of information regarding 17 entities and 44 individuals. The information obtained was used as part of 11 forms of operational work.

The Office of the Polish Financial Supervision Authority (UKNF) informed that in 2024 the GIFI provided 6 notifications to the Office of the Polish Financial Supervision Authority on reasonable suspicion of a breach of regulations related to the operation of the financial market. The Office of the Polish Financial Supervision Authority launched analytical activities in connection with the information received; however, these did not result in notifications to the public prosecutor's office.⁵⁵

⁵⁵ With regard to the human resources involved in the implementation of AML/CFT tasks, the Office of the Polish Financial Supervision Authority reported that it employed 26 persons directly involved in activities under the AML/CFT Act as of the end of 2024. These persons perform audit, supervisory, international and administrative tasks in the field of AML/CFT. Human resources and their adequacy for the duties assigned are subject to ongoing monitoring by the Office of the Polish Financial Supervision Authority. In view of the changes to the current legislation in terms of assigning new AML/CFT responsibilities to the Office of the Polish Financial Supervision Authority, expanding the catalogue of supervised obligated institutions and increasing the scope of control to include compliance with restrictive measures related to the Russian Federation's aggression against Ukraine and compliance with obligations to transfer recorded information to the Clearing House IT System (STIR), resulting from the provisions of the Act of 1 December 2022 on the Financial Information System, the Office of the Polish Financial Supervision Authority identifies the need to further strengthen the assets dedicated to these tasks. Despite the recruitment efforts of the Office of the Polish Financial Supervision Authority, the planned staffing levels were not achieved in 2024.

The President of the Supreme Audit Office communicated that in 2024 he had requested, pursuant to Article 105(3)(2) of the *AML/CFT Act* of 27 June 2024, that the documents and information necessary to carry out audit P/24/010 — Functioning of the system for counteracting money laundering and financing of terrorism — be made available to authorised auditors of the Supreme Audit Office. Audit P/24/10 used information and documents protected under the *AML/CFT Act*, which were made available to authorised auditors of the Supreme Audit Office in its course.

The National Centre for Emissions Management (KOBiZE) notified the GIFI that in 2024, it did not send any inquiries/requests for information to the GIFI under the *AML/CFT Act*.

6.3 DATA CONCERNING CRIMINAL PROCEEDINGS

Pursuant to Article 14(3) of the *AML/CFT Act*, the Minister of Justice is obliged to provide the GIFI with aggregate data on:

- the number of criminal proceedings initiated and completed in cases related to money laundering and on the number of criminal proceedings initiated and completed in cases related to financing of terrorism;
- the number of individuals that were presented with charges of money laundering and the number of individuals that were presented with charges of financing of terrorism;
- the number of individuals convicted by a final court judgement for money laundering and the number of individuals convicted by a final court judgement for financing of terrorism;
- the types of predicate offences referred to in Article 1(e) of the *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, done in Warsaw on 16 May 2005* (Journal of Laws of 2008, item 1028 and of 2018, item 1328), hereinafter referred to as the “Warsaw Convention”, to which the information indicated in the preceding subparagraphs refer;
- assets that were frozen or with respect to which transactions were suspended or accounts were blocked, or for which property searching, seizure or forfeiture was adjudicated.

According to the data provided by the Ministry of Justice, in 2024, regional and district courts initiated 454 court criminal proceedings against 1,383 individuals regarding an offence under Article 299 of the *Penal Code*. During the same period, the courts completed 244 criminal proceedings in cases regarding the aforementioned offence. According to the Ministry of Justice data, 2024 saw a total of 413 persons finally⁵⁶ sentenced for committing a money laundering offence under Article 299 of the *Penal Code*, with 575 sentenced in the first instance. In the course of these proceedings, property worth in total PLN 13,776 and assets worth PLN 31,000 were seized, as well as forfeiture was adjudicated with respect to property with a total value of PLN 188,305,403.

Information provided by the Ministry of Justice also shows that in 2024, common courts did not initiate any criminal proceedings regarding an offence under Article 165a of the *Penal*

⁵⁶ According to the information obtained from the Ministry of Justice, the data in this section is provided by the Divisions of the District Courts (first instance) and of the Regional Courts. What matters is whether the court judgement is final, not the instance at which it became final.

Code, and completed no criminal proceedings under this article. In 2024, 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 of terrorism.

Court criminal proceedings conducted in Poland in 2024 under Article 299 of the *Penal Code* related to the following predicate offences referred to in Article 1(e) of the Warsaw Convention:

- under the following articles of the *Penal Code*: Article 204 (pimping, coercing or taking advantage of the prostitution of others); Article 228 (passive bribery); Article 230a (paid active protection); Article 252 (hostage-taking); Article 258 (organised criminal group and criminal association); Article 263 (unlicensed manufacture or possession of weapon); Article 270 (substantive deceit); Article 271 (intellectual deceit); Article 271a (intellectual forgery of invoices); Article 272 (extortion of false statement); Article 278 (theft); Article 284 (misappropriation); Article 286 (fraud); Article 287 (computer fraud); Article 288 (destruction of property); Article 291 (intentional fencing); Article 296 (causing damage to business); Article 297 (credit fraud); Article 299 (money laundering); Article 300 (frustrating or reducing satisfaction of a creditor);
- under the following articles of the *Fiscal Penal Code*: Article 54 (failure to disclose the object or basis of taxation); Article 55 (untrue tax data); Article 56 (tax fraud); Article 56a (failure to submit vehicle information to the competent tax authority); Article 62 (breach of accounting procedure); Article 76 (unjustified tax refund);
- offences under the following articles of the *Act of 29 July 2005 on Counteracting Drug Addiction*: Article 53 (manufacture, processing, conversion of narcotic drugs, psychotropic substances or new psychoactive substances or processing of poppy straw); Article 54 (manufacture, possession, storage, disposal or acquisition of instruments); Article 55 (import, export, transport, intra-Community acquisition, intra-Community supply of narcotic drugs, psychotropic substances, new psychoactive substances or poppy straw); Article 56 (marketing of narcotic drugs, psychotropic substances, new psychoactive substances or poppy straw. Participation in trade); Article 61 (criminal acts involving precursors or new psychoactive substances); Article 62 (possession of narcotic drugs or psychotropic substances);
- other offences (*under the Penal Code and special acts*);
- other unspecified offences.

6.4. TRAINING ACTIVITY

In implementing the training programmes developed under Action No. 21 of the Action Plan of the 2021 National Strategy for Counteracting Money Laundering and Financing of Terrorism, the GIFI took measures to improve the knowledge of employees of obligated institutions and cooperating units in counteracting money laundering and financing of terrorism. As part of these activities, it conducted a series of training courses addressed to the employees of obliged institutions and cooperating units. The following training courses were conducted:

- Customer due diligence measures — their purpose, relation to the ML/TF risk assessment and scope. Politically exposed persons.

- Quarterly reporting to the GIFl by obligated institutions dealing with virtual currencies.
- Assessment of ML/FT risk: Identification and assessment of the ML/FT risk by obligated institutions. Identification and assessment of risks related to business relationships or occasional transactions. National ML/FT Risk Assessment and Supranational ML/FT Risk Assessment.
- Money laundering: risks arising from predicate offences.
- Suspicious Activity Report? — It's easy! How to skilfully improve reporting.
- Control of the fulfilment of AML/CFT obligations by obligated institutions.
- Consequences of failure to fulfil obligations provided for in the *AML/CFT Act*.
- Principles for applying the *AML/CFT Act* with particular reference to issues relating to auditing foundations to the extent indicated in the Act.
- Using non-financial sector companies in money laundering offences.
- Applying specific restrictive measures on terrorist financing and proliferation.
- Money laundering in theory and practice.

The programme trained a total of 23,675 personnel, including 11,853 from obligated institutions and 11,822 from cooperating entities.

The aforementioned training courses are held periodically, and the training topics will be repeated in subsequent years. Participation in training is free of charge, and obligated institutions and cooperating units can register an unlimited number of employees.

Cooperation with organisational units of the public prosecutor's office, involving the participation of representatives of the Department of Financial Information in initiatives aimed at exchanging experience in AML/CFT, continued in 2024. This made it possible to disseminate good practices aimed at ensuring a more effective interaction between the GIFl and representatives of organisational units of the public prosecutor's office.

On 13 September 2024, the 4th edition of the conference "What about this AML? What challenges do we face?" was held in Warsaw. Participants exchanged experiences, best practices and the latest trends in AML. The conference provided a platform to discuss effective strategies and innovative solutions in the field of AML. A representative of the GIFl gave a lecture entitled "AMLA and other international challenges in the area of AML/CFT" at the conference.

Between 30 September and 1 October 2024, a face-to-face meeting of the AML Forum at the Security Council of the Polish Bank Association was held in Warsaw, during which experts discussed significant changes for the banking sector in the context of the new EU AML package. The participants exchanged experiences and best practices in AML and cooperation with regulatory authorities. The forum featured a presentation by a GIFl representative, entitled "Significant changes for the banking sector in the context of the new EU AML package".

In 2024, a representative of the Department of Financial Information also participated in and led two training courses on:

- tax crime — training delivered to police officers by the Police Academy in Szczytno (November 2024);

- anti-money laundering — training delivered to police officers by the Police Academy in Piła (December 2024).

Representatives of the Department of Financial Information also participated in the third (June 2024) and fourth (October 2024) editions of the AML FORUM dedicated primarily to obligated institutions.

In May 2024, an DFI representative participated in and spoke at a conference called "Preventing TV Signal Theft", held at the Police Academy in Piła and co-organised by the SYGNAŁ Association.

In June 2024, a representative of the Department of Financial Information took part in the sixth edition of the ICT Crime XXI conference organised by the Polish Naval Academy in Gdynia, which focused on issues related to combating cybercrime. The event was co-organised by the Central Cybercrime Bureau.

Publication of the GIFI's typology newsletters

As part of sharing AML/CFT knowledge and information, the GIFI continued to regularly publish a typological newsletter throughout 2024. The newsletter is supposed to help obligated institutions recognise activities that may be related to ML/TF and broaden their general knowledge of counteracting these offences. The topics of the newsletters published in 2024 were selected based on the areas identified in the National Assessment of the Risk of Money Laundering and Financing of Terrorism as areas associated with higher ML/FT risk:

- Virtual asset service providers;
- Crowdfunding.

Newsletters can be downloaded after logging into an obligated institution account in the GIFI ICT System. Obligated institutions without access to that website may request the newsletter by emailing newslettergiif@mf.gov.pl. Information about subsequent issues of the typological newsletter is published in the form of a message on the GIFI's website.

Conference for entities cooperating in the application of the AML/CFT Act, co-organised with the Central Register of Beneficial Owners (CRBR), 11–13 September

On 11–13 September 2024, the Tax Administration Chamber in Bydgoszcz hosted a three-day conference called "Activities of Cooperating Units under the *Act on Counteracting Money Laundering and Financing of Terrorism*", organised in cooperation with the GIFI. The conference was attended by representatives of services, institutions and bodies operating in the field of AML/CFT and counteracting predicate offences (Central Anti-Corruption Bureau, Internal Security Agency, Central Bureau of Investigation, Military Police, Border Guard, the Police, National Revenue Administration, Ministry of Finance, Polish Financial Supervision Authority and National Bank of Poland). The participants discussed various aspects of the activities, including cooperation in combating money laundering and the financing of terrorism. At the invitation of the GIFI, the conference was attended by representatives of foreign administrative authorities (Czech Republic, Malta and Latvia) handling tasks related to maintaining registers of beneficial owners.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with the European Commission

7.1.1. Expert Group on Money Laundering and Terrorist Financing

Expert Group on Money Laundering and Terrorist Financing

The *Expert Group on Money Laundering and Terrorist Financing* (EGMLTF), bringing together representatives of the EU Member States, is to support the European Commission in defining policy directions in the area of counteracting money laundering and financing of terrorism, developing legal acts, as well as providing advice at the stage of preparing proposals on implementing measures and coordination of cooperation between EU Member States.

In 2024, the GIFI representatives participated in three online EGMLTF meetings. The meetings covered topics related to the internal affairs of the European Union and external affairs within the framework of international cooperation.

As regards the internal affairs, the meetings were dedicated mainly to:

1. The AML/CFT Package, including:
 - the AMLA Task Force;
 - the transnational risk assessment at Union level in 2028 under Article 7 of Directive (EU) 2024/1640;
 - the preparation of legislation at second and third level under the new legal framework;
 - transposition workshops on the AML/CFT Package;
2. The implementation of tasks under the current AML framework and the AML/CFT Action Plan, including:
 - the central database on AML/CFT and the regulatory technical standards of the European Banking Authority;
 - enforcement and effective implementation of Directive (EU) 2015/849;
 - the AML Technical Support Facility;
 - the Single List of Politically Exposed Persons;
 - the 2025 Supranational ML/TF Risk Assessment;
 - the preparation of a report to the European Parliament and the Council under Article 65 of Directive 2015/849;
 - statistics in accordance with Article 44 of Directive 2015/849;
 - the implementation of the EU FIUs Platform work plan for 2022–2024.

Discussions also concerned the document prepared by the Directorate-General for Migration and Home Affairs (HOME) on the link between citizenship programmes in exchange for investment, as offered by third countries benefiting from visa liberalisation, and economic crime — particularly money laundering and the financing of terrorism.

The Commission also organised a presentation for various national authorities, including Financial Intelligence Units, presenting the preferred technical solution for establishing the Bank Account Registers Interconnection System (BARIS), through which it is required under Directive (EU) 2024/1640 to integrate centralised automated mechanisms by 10 July 2029.

The Commission also provided advice on completing the FATF questionnaire on the status of implementation of Recommendation 15 by FATF members and jurisdictions where virtual asset service providers are particularly active.

With regard to external affairs, in preparation for the FATF and MONEYVAL plenary meetings, issues relating to AML/CFT national system assessments and projects being carried out and planned for implementation by working groups within these fora were discussed.

Further, like in previous years, in 2024 EGMLTF members were consulted by written procedure on a draft Commission Delegated Regulation amending Delegated Regulation (EU) 2016/1675 on the list of high-risk third countries and on a questionnaire to collect statistics related to the effectiveness of member states' AML/CFT regimes.

The GIFI also worked with the Commission in 2024 to develop the programme for a seminar on the implementation of the AML/CFT legislative package, organised by Poland as part of its Presidency of the EU Council on 27–28 March 2025.

7.1.2. EU-FIU Platform

In 2024, the GIFI representatives actively participated in the work of the EU-FIU Platform. The purpose of the platform is to provide the Commission with advice and knowledge of national experts, facilitate cooperation between Member States' FIUs, and exchange information on, among others, trends and factors relevant to the assessment of ML/FT risks at national and supranational level, as well as the identification of suspicious cross-border transactions. In 2024, four regular meetings of the EU-FIU Platform were held (including two ones in the form of video conference).

In particular, the implemented tasks included supporting the European Commission in preparing regulations related to establishing the Anti-Money Laundering and Countering the Financing of Terrorism Authority (AMLA), as well as defining strategies, priorities and medium- and long- term plans for the development of the FIU.net, the EU system for the exchange of information among FIUs.

Members of the EU-FIU Platform listened to presented information and held discussions on:

- the formation of the AMLA, based in Frankfurt am Main, and the creation and operation of the AMLA Task Force;
- the provisions of Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849;
- further sanctions packages against the Russian Federation;

- financial crime threats in the EU, related to schemes to obtain citizenship through investment;
- the detection and reporting of suspicious transactions;
- the activities of the project team responsible for providing a data analysis tool for AMLA;
- the projects under the European Commission's Technical Support Instrument — 23 projects focused on anti-money laundering and counter-terrorist financing, as well as 11 projects focused on sanctions issues.

7.2. Cooperation with the Council of the EU

In 2024, during the Belgian and then Hungarian presidencies of the Council of the EU, the final pieces of legislation, part of the AML/CFT Package presented by the European Commission in July 2021, were adopted and published. Further, they consulted with representatives of the GIFI on the translation of these legal acts into Polish.

In 2024, the GIFI continued its activities in preparation for the Polish Presidency of the EU Council in the first half of 2025. These included the participation of the GIFI representatives in a series of training sessions for members of the presidency corps and the preparation of a seminar on the implementation of the AML/CFT Package, to be held on 27–28 March 2025.

7.3 MONEYVAL Committee

Participation in the work of the MONEYVAL Committee

In 2024, the following activities were carried out as part of participation in the work of the MONEYVAL Committee:

Plenary meetings of the MONEYVAL Committee: a Polish delegation composed of representatives of the GIFI, the Financial Supervisory Authority and the National Public Prosecutor's Office participated in the plenary meetings of the MONEYVAL Committee. The meetings took place on 21–24 May 2024 and 2–6 December 2024.

MONEYVAL member states' mutual *AML/CFT system* evaluation reports: a mutual evaluation report on Jersey was adopted at the plenary meeting in May 2024, followed by a mutual evaluation report on Bosnia and Herzegovina in December. Both countries have been included in the standard progress reporting procedure, which means that they will report on their progress in implementing international *AML/CFT* standards in two years' time.

1. Progress reports:

- The following progress reports were adopted: Hungary (6th Progress Report), Gibraltar (2nd Progress Report), Slovakia (3rd Progress Report) and Estonia (1st Progress Report);
- The progress reports for Georgia, Croatia, Poland, Estonia and Monaco were approved through written procedures;
- It was agreed to remove Armenia, Albania, the Czech Republic, Hungary, the Isle of Man, Andorra and Lithuania from the compliance monitoring process,

which indicates significant progress by these countries in implementing the recommendations of experts of the MONEYVAL Committee.

2. Compliance monitoring procedures:

- A warning was issued to Moldova to take more intensive action to address the shortcomings identified during the fifth round of mutual evaluations. The first step of the compliance procedure will be taken against Moldova automatically if it does not demonstrate sufficient progress in addressing the deficiencies by June 2025.
- In May 2024, the FATF acknowledged Gibraltar's progress in ensuring compliance with the FATF Recommendations and decided to take it out of the enhanced monitoring procedure.
- Typological projects: in 2024, the MONEYVAL Committee worked on the following typological projects: "Proceeds and conflict", chaired by Ukraine, and "Practice of Using Virtual Assets, Virtual Asset Service Providers & Platforms in the Laundering of Criminal Property", chaired by the Isle of Man.
- Training and cooperation: two training courses for evaluators were held to prepare them to conduct evaluations as part of the 6th round of member state mutual evaluations. A training course was organised in Helsinki in January and another one in Riga in May. Representatives of Poland, including the GIF, participated in the trainings.
- Cooperation with the FATF: a MONEYVAL delegation participated in FATF meetings, discussing common priorities and strategic issues in the global *AML/CFT system*. These activities underline MONEYVAL's commitment to the global *AML/CFT* network.
- As of 1 June 2024, Mr Lado Lalicic has been appointed as Executive Secretary of the MONEYVAL Committee.

Progress Report for Poland

In 2024, Poland was evaluated in terms of its progress in implementing the recommendations of MONEYVAL Committee evaluators, as contained in the evaluation report published in December 2021 on the MONEYVAL Committee website⁵⁷.

After analysing the adjustments made in April 2024, Poland submitted a request to the MONEYVAL Secretariat to upgrade its assessment for Recommendation 1 (Assessing risks and applying a risk-based approach), Recommendation 15 (New technologies), Recommendation 26 (Regulation and supervision of financial institutions) and Recommendation 33 (Statistics). In June 2024, Poland submitted to the MONEYVAL Secretariat a completed follow-up report questionnaire on these recommendations as well as relevant information and additional materials.

At the MONEYVAL Committee meeting in December 2024, the MONEYVAL Committee, under a written procedure without plenary discussion, accepted Poland's request to upgrade the

⁵⁷ <https://rm.coe.int/moneyval-2021-25-mer-pl-en/1680a55b9a>

rating for Recommendations 1 and 33 to LC (largely compliant) while maintaining those for Recommendations 15 and 26 at PC (partially compliant), arguing that Poland's progress was still insufficient. As a result of the changes in the compliance assessment, 14 out of 40 FATF Recommendations remain rated at PC level.

The rating for Recommendation 1 was improved thanks to the development and publication on the Public Information Bulletin (BIP) website in December 2023 of a new National Assessment of the Risk of Money Laundering and Financing of Terrorism. In addition, the improvement in the compliance assessment was the result of adjustments (as part of the implementation of the [2021 AML/CFT Strategy](#)) to the resources of certain institutions responsible for combating money laundering and the financing of terrorism. The GIFI training activities and the implementation of the TSI project "Strengthening the risk assessment mechanisms and the AML-CFT strategic analysis function of the Polish Financial Intelligence Unit" also had a positive impact on the assessment.

The increase in the rating for Recommendation 33 was due to the activities of the Polish authorities in collecting statistics enabling the measurement of the effectiveness of [AML/CFT](#) measures. The GIFI introduced system changes enabling the division of received notifications on suspicious activity into ML notifications and FT notifications.

Regarding Recommendation 15, it is worth noting that the partial marks for selected criteria under this recommendation have been raised. The Polish [AML/CFT](#) system still lacks specific requirements for obligated institutions regarding the assessment of ML/FT risks associated with new technologies, products or services prior to their introduction to the market. However, supervisory activities of the GIFI and the Office of the Polish Financial Supervision Authority (training, periodic reporting, guidelines, announcements, newsletters) encouraging institutions to consider new risk factors in their risk assessments, including new technologies, were noted. As for Virtual Asset Service Providers (VASPs), while they have been recognised as obliged institutions, the risks associated with their activities are included in the NRA and there is an obligation to register them, the money remittance requirements of FATF Recommendation 16 have still not been implemented for them, and the definition of VASPs in the [Polish AML/CFT Act](#) is not fully in line with the FATF definition.

In the context of Recommendation 26, ratings for some criteria have also been upgraded. Still, the shortcomings that prevent a higher rating include not treating value transfer providers as a separate category of obligated institutions and gaps in the market entry requirements meant to stop criminals from using financial institutions. Furthermore, the elements of risk-based supervision are not sufficiently defined and the supervisors (the GIFI, National Bank of Poland, Office of the Polish Financial Supervision Authority) have not included the frequency of supervisory activities in their control methodology or annual control plans.

Horizontal Study — EU Supranational Measures in MONEYVAL Fifth Round Mutual Evaluation Reports

In 2023-2024, a GIFI representative was a member of the project team preparing a horizontal report analysing how transnational legislation, mechanisms and other EU initiatives were taken into account and assessed in the 5th round of MONEYVAL Mutual Evaluation. In addition to the Polish representative, the team included staff from the MONEYVAL Secretariat. This

served to implement one of the objectives set in the MONEYVAL Strategy for 2023–2027, adopted in April 2023.

The analysis contained in the report will help to develop a better understanding and more coherent assessment of the supranational mechanisms applied in the EU Member States, subject to mutual evaluation by the MONEYVAL Committee.

The report was adopted at the 68th Plenary Meeting and published on the MONEYVAL Committee website.

Participation in evaluations of MONEYVAL Committee member states

In 2024, representatives of Poland (the GIFİ and Office of the Polish Financial Supervision Authority) continued to work as evaluators in the evaluation processes of the *AML/CFT* systems of Jersey and Bosnia and Herzegovina. The evaluation reports of these countries were adopted at the plenary meetings of the MONEYVAL Committee in May and December 2024, respectively.

In December 2024, representatives of Poland (GIFİ and Office of the Polish Financial Supervision Authority) commenced work to contribute to an assessment of Romania's progress in implementing the recommendations from the 5th round evaluation report on ensuring technical compliance with FATF Recommendations. The Polish reviewers are tasked with analysing the materials submitted by Romania and preparing proposals for comments on Romania's first progress report. The report will be adopted at the plenary meeting in May 2025.

Elżbieta Franków-Jaśkiewicz honoured in the project "75 women in 75 years of Council of Europe history"

In June 2024, the GIFİ representative Elżbieta Franków-Jaśkiewicz was recognised by the Council of Europe, together with the European Union Delegation to the Council of Europe and the Permanent Representations of the Kingdom of the Netherlands and the United Kingdom, in the project "75 women in 75 years of Council of Europe history".

Elżbieta Franków-Jaśkiewicz is one of the most active women in the global *AML/CFT* network. She has promoted the work of the Council of Europe in preventing and combating money laundering and the financing of terrorism, both at European and global level. She was the first female chair of the MONEYVAL Committee. More recently, she was involved in the negotiation and adoption of the "MONEYVAL Committee Strategy for 2023–2027".

7.4. Conference of the States Parties to the Warsaw Convention

In connection with the implementation of the Warsaw Convention and Poland's participation in the COP, the GIFİ continued its actions related to the activities of this forum. The 16th COP Plenary Meeting took place on 17–18 October 2024.

During the meeting, the importance of the Convention and its role in international cooperation was emphasised.

States were encouraged to reduce the number of reservations to individual articles of the Convention. The withdrawal of reservations by Slovakia to the Convention's Article 7(2c) (Monitoring of banking operations) and by Slovenia to Article 3(4) (Reversed burden of proof)

was particularly welcomed. In Poland, according to information provided by the Ministry of Justice prior to the COP meeting, the review of reservations and declarations submitted to the Convention in the field of criminal law has been completed and work is underway to prepare a draft law that will allow these reservations to be withdrawn.

The COP was asked by the Committee of Ministers of the Council of Europe to give its opinion on Kazakhstan's application to join the Convention. After analysing its compliance with international conventions, delegations did not oppose this application and proposed a review of Kazakhstan's compliance with the Convention.

During the meeting, progress was presented on the draft additional protocol to the Convention, which covers issues such as confiscation without a conviction and the establishment of national agencies to manage confiscated property.

The plenary session also adopted amendments to the interpretative note to Article 11 of the Convention. The COP's scientific expert explained that while judges are not obliged to recognise previous foreign judgments, the national legal order should nevertheless provide for such an option and that the legal possibility of not imposing a more severe penalty in the absence of foreign recidivism is not covered by Article 35 of the Convention.

Changes to the FATF standards Recommendation 4 (Confiscation and provisional measures), Recommendation 30 (Responsibilities of law enforcement and investigative authorities), Recommendation 31 (Powers of law enforcement and investigative authorities), Recommendations 38 (Mutual legal assistance: freezing and confiscation) and 40 (International cooperation), and Direct Outcomes 2 (Effective international cooperation) and 8 (Effective asset recovery) were also discussed.

During the meeting, a discussion took place on the assessment of the degree of implementation by Morocco and Aruba of those provisions of the Convention that have been the subject of thematic COP monitoring reports since 2018. It was agreed that these countries would be included in the work plan for the next horizontal reports on articles that had not been implemented at a satisfactory level.

The progress made by the following countries was analysed:

- Montenegro, Russian Federation, Serbia and Turkey — with regard to the implementation of the Convention's Art. 11 (International recidivism);
- Armenia and Serbia — with regard to the implementation of the Convention's Art. 25(2) and (3) (Priority of return of confiscated property to the requesting party and consideration of agreements on the return of confiscated property);
- North Macedonia — with regard to the implementation of the Convention's Art. 25(2) (Priority for return of confiscated property to the requesting party);
- Russian Federation — with regard to the implementation of the Convention's Art. 14 (Postponement of suspicious transactions).

For countries that have not shown sufficient progress, consultative meetings were scheduled with the Chair, Vice-Chair or member of the COP Office, the head of the delegation or permanent representation of the country concerned and interested experts to encourage priority implementation of the actions recommended as a result of the horizontal reviews.

Moreover, the Secretariat analysed the progress made by Denmark, France, Lithuania, Monaco and Spain in implementing Articles 7(2c) and 19(1) of the Convention. The report noted the progress of Lithuania and Monaco. Countries that do not meet the objectives of the aforementioned articles will submit the relevant reports in 2025.

7.5. Egmont Group

In 2024, the Polish Financial Intelligence Unit continued its work within the Egmont Group, which brings together 177 financial intelligence units from around the world, participating in work, initiatives and meetings at the working and plenary levels.

The GIFI representatives participated in meetings of the Working Group on Information Exchange and the Technical Assistance and Training Working Group, as well as the Europe 1 Regional Group, and were involved in cooperation with the Egmont Group Secretariat. They also participated in the 30th Plenary Meeting and the meeting of the Heads of Financial Intelligence Units.

The 2024 Egmont Group Working and Regional Group Meetings were held from 29 January to 2 February 2024 in Malta. The event was hosted by the Financial Intelligence Unit of Malta (FIAU).

The following were discussed during the meetings:

- progress on the Egmont Group Strategic Plan 2022–2027;
- strengthening the organisation by reviewing and approving the membership of new FIUs and appointments to certain leadership positions in it;
- the needs of Egmont Group FIUs in terms of training and technical assistance, and proposals for initiatives to meet these needs;
- the current risks in the areas of money laundering and the financing of terrorism, including the role of the FIUs in the asset recovery process, in preventing the evasion of sanctions used to counter the financing of the proliferation of weapons of mass destruction and in preventing the misuse of non-profit organisations to finance terrorism;
- Egmont Group's operational and strategic objectives;
- opportunities for further use of new technologies to accelerate information sharing by FIUs, including cloud-based services and advanced IT analytical tools.

As regards regional group meetings, the GIFI representatives are involved in the activities of the Europe I region, which comprises the Financial Intelligence Units of the European Union member states. During the 2024 meetings, the discussions of the units from this region focused on issues related to preparations for the implementation of legal acts adopted by the European Union as part of the [AML/CFT](#) package, including AMLA, the delegation of employees by Financial Intelligence Units to AMLA, future joint analyses and IT tools supporting these analyses.

A plenary meeting of the Egmont Group was held from 2 to 7 June 2024 in Paris. The main topic of the meeting was the development of the concept of the Next Generation FIU, which supports the implementation of the Egmont Group Strategic Plan 2022–2027. The discussion

focused on three topics: the development of FIU staff, the use of new technologies by FIUs, as well as the role of FIUs in combating new types of crime.

During the plenary session, representatives of the FIUs, after hearing the recommendations of the Egmont Group advisory panel, elected Ms Elżbieta Franków-Jaśkiewicz, Deputy Director of the Department of Financial Information, as the new Chair of the organisation. Ms Elżbieta Franków-Jaśkiewicz has served as interim Chair of the Egmont Group since September 2023, having previously served as Vice Chair of the Group. The new Chair listed the following among her priorities for her two-year term:

- ensuring transparent procedures to promote trust in the Egmont Group,
- using innovative approaches to strengthen cooperation with key Egmont Group partners (FATF, FATF-style regional bodies, G20, OECD, Council of Europe),
- increasing active participation of FIU representatives in the work of the Egmont Group,
- pursuing asset recovery priorities by encouraging FIUs to accede to the Warsaw Convention and its Additional Protocol,
- strengthening cooperation between FIUs and *AML/CFT* Supervisory Authorities,
- improving cooperation between customs authorities and FIUs.

The plenary also featured the Best Egmont Case Award (BECA) competition. Its aim is to recognise FIUs that have contributed to successful investigations of money laundering or terrorist financing through the exchange of information.

ECOFEL WORKSHOP

The Egmont Centre of FIU Excellence and Leadership (ECOFEL), in cooperation with Department of Financial Information, organised a workshop within the operational group on Virtual Assets (Virtual Assets Operational Taskforce - VASP) in Poland on 13–15 March 2024, targeted at Ukrainian partners (also with the participation of representatives of FIUs of selected member countries of the taskforce). The workshop focused on the issues of circumventing sanctions using cryptocurrencies and crypto-asset providers. During the training, participants were able to learn about some aspects of terrorist financing, tools for analysing data related to cryptocurrency flows, as well as to exchange experiences from ongoing analyses of crypto-asset flows originating from illegal activities.

7.6. Financial Action Task Force

Plenary meetings of the Financial Action Task Force (FATF) and FATF working group meetings were held in Paris on 19–23 February and 21–25 October 2024 and in Singapore on 24–28 June 2024. While Poland is not a member of the FATF, it nonetheless participates in its work as part of the MONEYVAL Committee delegation, as well as through the GIF representative's role as Chair of the Egmont Group.

In 2024, the FATF updated the list of jurisdictions subject to enhanced monitoring (the so-called FATF grey list), adding Kenya and Namibia (in February 2024), Monaco and Venezuela (in June 2024) as well as Algeria, Angola, Lebanon and Côte d'Ivoire (in October 2024). In turn, Barbados, Gibraltar, Uganda and the United Arab Emirates (in February 2024), Jamaica

and Turkey (in June 2024) and Senegal (in October 2024) were removed from the list. These countries have demonstrated progress in addressing strategic deficiencies and will work with relevant FATF-style regional bodies to further strengthen their [AML/CFT/CFP](#) systems.

In 2024, the FATF approved revised criteria for the prioritisation of countries in the review process of the Financial Action Task Force (FATF). The International Cooperation Review Group (ICRG) has identified countries with strategic deficiencies in counteracting money laundering and financing of terrorism that pose a risk to the international financial system (countries on the FATF "grey list" or "blacklist"). These criteria will be applied in the next round of mutual evaluations. They are intended to ensure that the FATF listing process remains risk-based, fair, transparent and sensitive to the challenges faced by least developed countries.

June 2024 saw the adoption and publication of the joint report of the FATF, the Asia/Pacific Group on Money Laundering (APG) and the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) on the evaluation of India's [AML/CFT/CFP](#) system, and the joint report of the FATF and the Middle East and North Africa Financial Action Task Force (MENAFATF) on the evaluation of Kuwait's [AML/CFT/CFP](#) system. In October, the last two mutual evaluation reports of the fourth round of FATF evaluations were adopted and published: the joint FATF/Financial Action Task Force of Latin America (GAFILAT) mutual evaluation of Argentina, as well as the joint FATF/MENAFATF mutual evaluation of Oman.

In the context of the Russian Federation, the FATF expressed concern about the growing threats to the international financial system arising from the actions of the Russian Federation and decided to maintain the suspension of its membership of the FATF.

In addition, the following activities were carried out as part of continued activity on FATF strategic initiatives:

- In November 2024, the FATF published revised guidance on national money laundering risk assessment. Work is underway on a comprehensive update of the requirements for terrorist financing risk assessment.
- The FATF continued its work on revisions to Recommendation 8: in February 2024, changes to the assessment methodology for the next round of peer reviews were agreed, which clarify existing obligations to apply risk-based measures to protect NPOs that are most vulnerable to potential terrorist financing abuse and prevent unintended consequences of misapplication of FATF requirements. The FATF has also embarked on a project to review its processes to ensure that countries are not misusing FATF requirements to restrict the activities of NPOs.
- In July 2024, the FATF published its fifth annual update on progress in countries' implementation of standards on virtual assets and virtual asset service providers. The aim of the initiative is to enable the FATF community to support jurisdictions in regulating and supervising virtual asset service providers and to encourage jurisdictions to fully implement Recommendation 15.
- A review (including through a public consultation) of standards for cross-border payment systems (Recommendation 16) was underway to make them faster, cheaper and more transparent, while ensuring compliance with [AML/CFT](#) requirements.

- Updated FATF guidance on a risk-based approach to Recommendation 25 on transparency and beneficial owners of legal arrangements was adopted in February 2024, which takes into account input from the public consultation announced after the FATF Plenary Meeting in October 2023. The initiative aims to facilitate the detection of corruption and the avoidance of sanctions via legal persons.
- The FATF conducted and published a horizontal review of member states' efforts to prevent the use of "gatekeepers", e.g. accountants, lawyers, real estate agents, to facilitate money laundering and the financing of terrorism.
- A collaborative project has been launched with data protection and privacy experts, the private sector and other international partners on information sharing under various national *AML/CFT/CFP* and data protection and privacy laws.
- The "Women in FATF and the Global Network (WFGN)" initiative to promote women in the fight against financial crime continued. This included launching the *"Breaking Barriers: Inspiring the Next Generation of Women Leaders"* e-book to inspire women to get involved in countering financial crime, as well as the second edition of a mentoring programme to strengthen inclusivity and diversity within FATF and the Global Network. The e-book also includes a contribution from the GIFI representative, Ms Elżbieta Franków-Jaśkiewicz, who shared her experience accumulated as Chair of the MONEYVAL Committee and the Egmont Group.

The FATF appointed Elisa de Anda Madrazo of Mexico as the new FATF President for the July 2024–June 2026 term. Key priorities of the Mexican Presidency include:

- Fostering financial inclusion by promoting risk-based implementation of the FATF Standards in line with the principle of proportionality;
- Ensuring the successful launch of a new round of mutual evaluations;
- Strengthening the coherence of the Global Network by promoting transparency, inclusion and unity, as well as supporting proposals to enhance cooperation between the FATF and FATF-style regional bodies;
- Supporting the effective implementation of the revised FATF Standards with a focus on asset recovery, beneficial owners and virtual assets; and
- Continuing efforts to combat terrorist financing and proliferation financing.

During the past year, the GIFI representatives participated not only in FATF meetings but also in its other activities.

Meetings of the Joint Groups under the ICRG

In 2024, the GIFI representatives attended two meetings of the Eurasia Joint Group (EE JG) functioning under the International Cooperation Review Group (ICRG) of the Financial Action Task Force (FATF), and one meeting of the E-MENA Joint Group (E-MENA JG). This was the inaugural meeting of the now merged groups, previously operating separately as the Eurasia Joint Group and the Middle East and North Africa Joint Group (MENA JG).

The E-MENA Joint Group comprises its co-chairs, representatives of the FATF Secretariat, the Middle East and North Africa Financial Action Task Force (MENAFATF) and the

MONEYVAL Committee, as well as experts reviewing the reports of the countries under review (*lead reviewers*) and national delegates.

At all meetings of the Joint Group, members met directly with delegations from each country covered by an ICRG review process to inquire about their systems for counteracting money laundering and financing of terrorism and the progress they were making in implementing their action plans with FATF. The GIFI representative participated as an expert, reviewing Monaco's report.

Participation in FATF training courses

From 2 to 5 July 2024, the GIFI representative participated in the Financial Action Task Force (FATF) "*ICRG Reviewer Training*", conducted by the FATF Training Institute in Busan, South Korea. The training course aims to prepare a group of experts who review country reports for a new round of assessments of AML/CFT regimes under the ICRG — the FATF's key process for verifying countries' compliance.

Representatives of the GIFI and the National Prosecutor's Office participated in training courses organised or co-organised by the FATF to prepare for the role of evaluators in the next round of countries' mutual evaluations regarding compliance of their *AML/CFT* systems with international standards.

Promoting FATF activities

As part of the GIFI's regular efforts to promote FATF initiatives at the national level, the GIFI kept the FATF informed of FATF activities, published information on FATF letters (including translations of FATF statements into Polish), as well as reports, FATF documents and FATF-led public consultations.

7.7. Eurasian Group on Combating Money Laundering

Since 2007, Poland has been an observer in the Eurasian Group on Combating Money Laundering (EAG), which is one of the so-called FATF-style regional bodies and an associate member of the FATF. The primary objective of the EAG is to protect the integrity of the global financial system by ensuring consistent implementation of FATF recommendations by countries in the Eurasian region. In practice, the Russian Federation plays a leading role in the work of this organisation, and as such, Poland has not actively engaged in activities related to its observer role in the Group since Russia's aggression against Ukraine.

7.8. Counter ISIS Finance Group

The participation of the GIFI representatives in the work of the *Counter ISIS Finance Group* (CIFG), a working group of the Global Coalition dedicated to combating ISIS financing, confirms Poland's role and involvement in the coordinated activities of the international community in this area. The group was established in 2015. It currently brings together some 70 countries and international organisations and coordinates action against ISIS financial support networks around the world. It is co-chaired by representatives of Saudi Arabia, the United States and Italy.

Two CIFG meetings were held in 2024, attended by representatives of more than 40 member states from around the world. The GIFI representative attended the meetings online. The meetings focused on the ways in which ISIS is being funded and combated across Asia and Africa. Representatives of CIFG member states and independent experts shared information on current sources and methods of funding for ISIS, presented case studies on ongoing actions against ISIS, showing, among other things, how coordinated action and information sharing between states and with the private sector, including non-profit organisations, is effectively strengthening efforts to counter ISIS. In particular, the case studies presented at the meetings dealt with the disclosure and disruption of ISIS transactions carried out outside the formal financial system, including through the hawala system and "cash couriers", using the non-profit sector as well as virtual assets and mobile payment systems.

The CIFG meetings also served as a means for the international community to work more closely with countries that are vulnerable to exploitation by ISIS financiers, with a view to enhancing the capacity of these countries to investigate, apply financial sanctions against ISIS-linked individuals and take other action against ISIS financing, as well as to assist jurisdictions with deficiencies in their *AML/CFT* systems to ensure compliance with international FATF standards in this area.

7.9 BILATERAL COOPERATION

7.9.1. BASIS OF INFORMATION EXCHANGE WITH FOREIGN FIUs

Memoranda of understanding on the exchange of information in the area of combating money laundering and financing of terrorism, and cooperation undertaken thereunder, correspond to the provisions of *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism*, of 16 May 2005, i.e. the Warsaw Convention (CETS 198), as well as standards developed in this area by the Egmont Group. The scope of the information received and made available, particularly additional information, depends each time on the scope of the inquiry and compliance with the fundamental provisions of the national law.

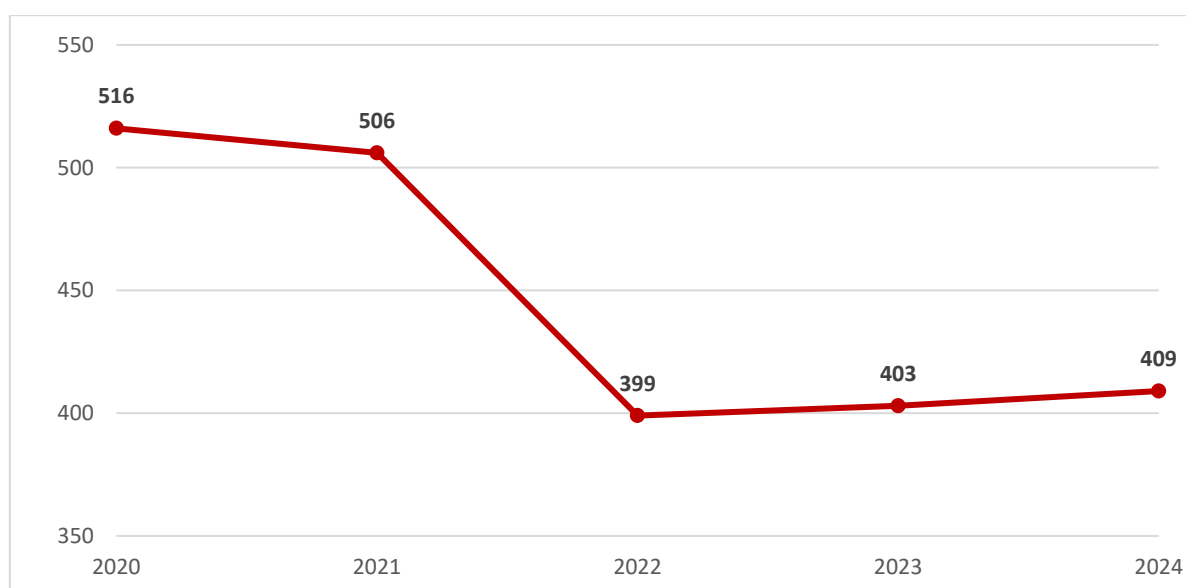
In the current legal situation, the GIFI's cooperation in the exchange of financial information related to counteracting money laundering and financing of terrorism with EU countries is regulated by Article 111(1) of the *AML/CFT Act*. Pursuant to Article 111(2) of the *AML/CFT Act*, the GIFI makes its financial information available to FIUs from non-EU countries on a reciprocal basis, and the exchange of information under the Warsaw Convention is regulated by Article 111(3) of the *AML/CFT Act*. Thus, in 2024 the GIFI did not sign any further memoranda of understanding on the exchange of information on counteracting money laundering and financing of terrorism.

7.9.2 EXCHANGE OF INFORMATION WITH FOREIGN FINANCIAL INTELLIGENCE UNITS

Requests and Information received by the GIFI from foreign partners

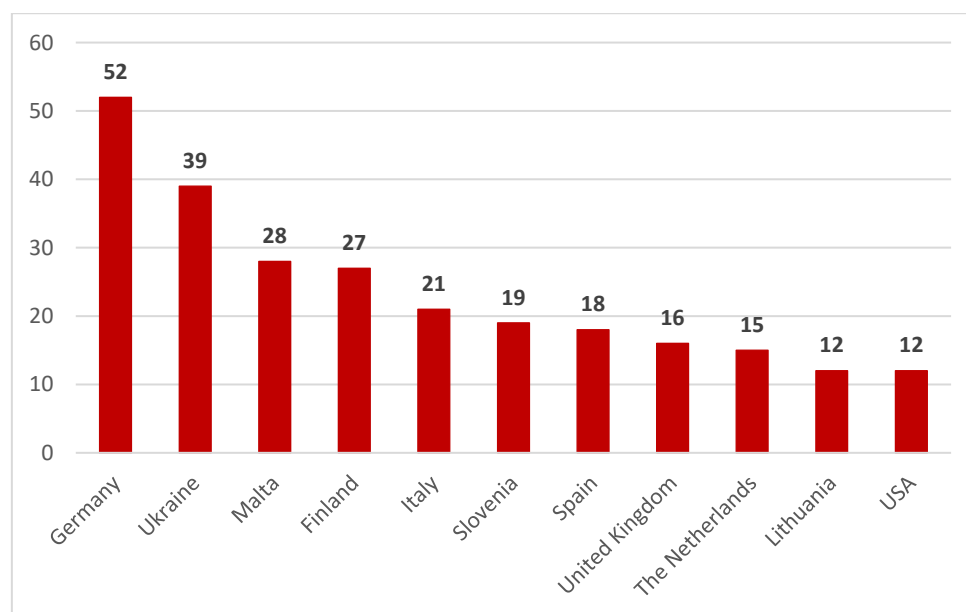
In 2024, the GIFI received 409 requests from foreign FIUs, which concerned a total of 2017 entities. This represents a slight increase in the number of requests compared to the previous year. The GIFI responded to all requests.

Chart 16. Inquiries from foreign FIUs in 2020-2024



About 68% of the inquiries came from FIUs of the EU member states. The GIFI received the largest number of enquiries from the FIUs of Germany, Malta and Finland. As for FIUs from non-EU countries, the largest number of requests for information were submitted to the GIFI by Ukraine, the United Kingdom and the USA.

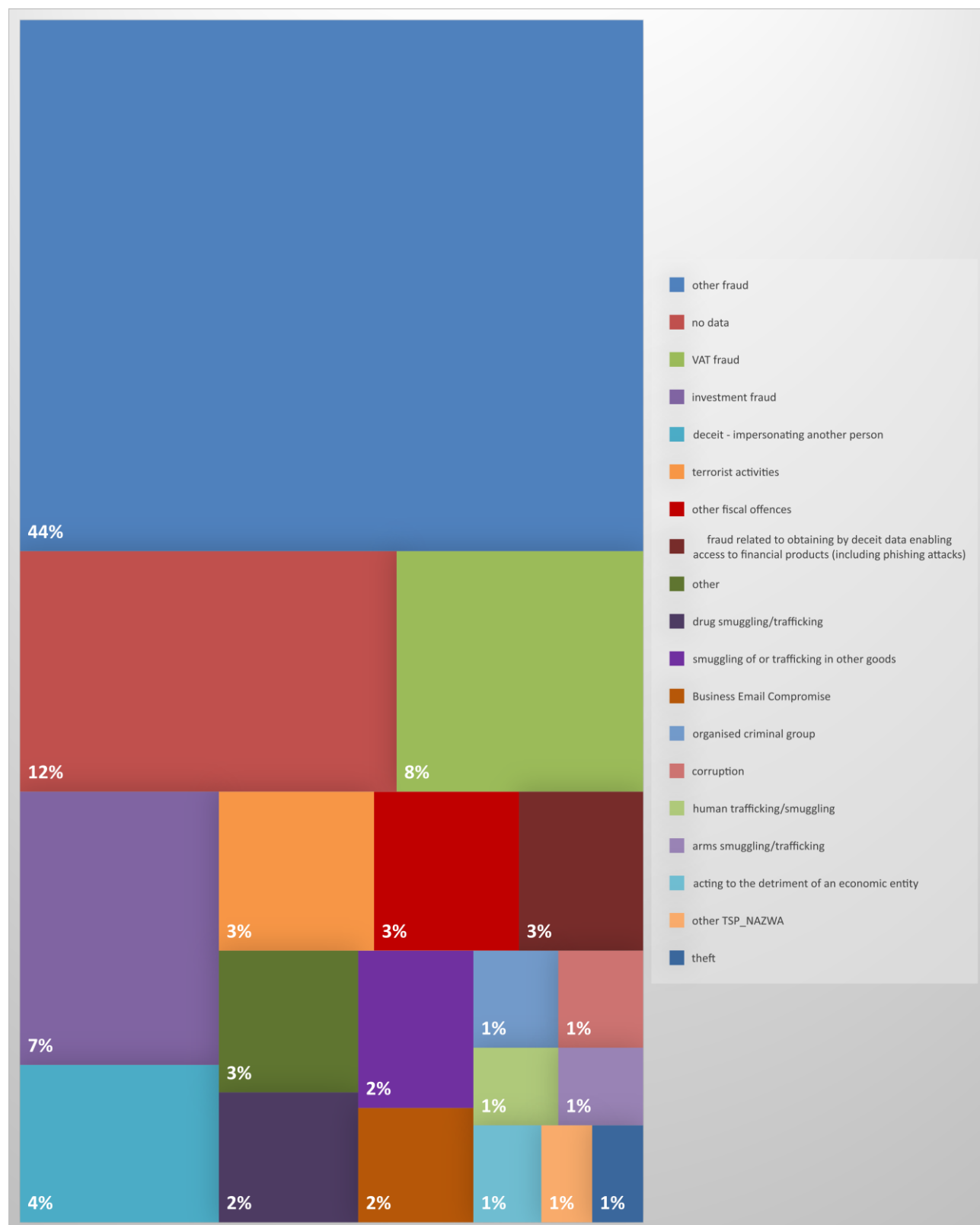
Chart 17. Top 10 countries from which foreign FIUs sent the largest numbers of inquiries in 2024



Of the 409 requests received from foreign FIUs, almost all, i.e. 400 requests, pointed to a potential money laundering offence. In 55 cases (12%), the predicate offence was not identified, indicating only possible links to money laundering. The most frequently identified predicate offence category was various types of fraud, which appeared in 201 applications, accounting for a total of 44% of all indications. Further, VAT fraud was explicitly mentioned for 8% of indications. Investment fraud accounted for 7% of indications, while deceit and fraud related to obtaining data enabling access to financial products (e.g. phishing) accounted for 4% and 3% of indications, respectively. Links to the potential financing of terrorism accounted for 3% of

the inquiries received (15 requests). Apart from the predominant various types of fraud and extortion, smaller but equally important categories such as organised crime, drug trafficking, human trafficking and economic crime are also noticeable.

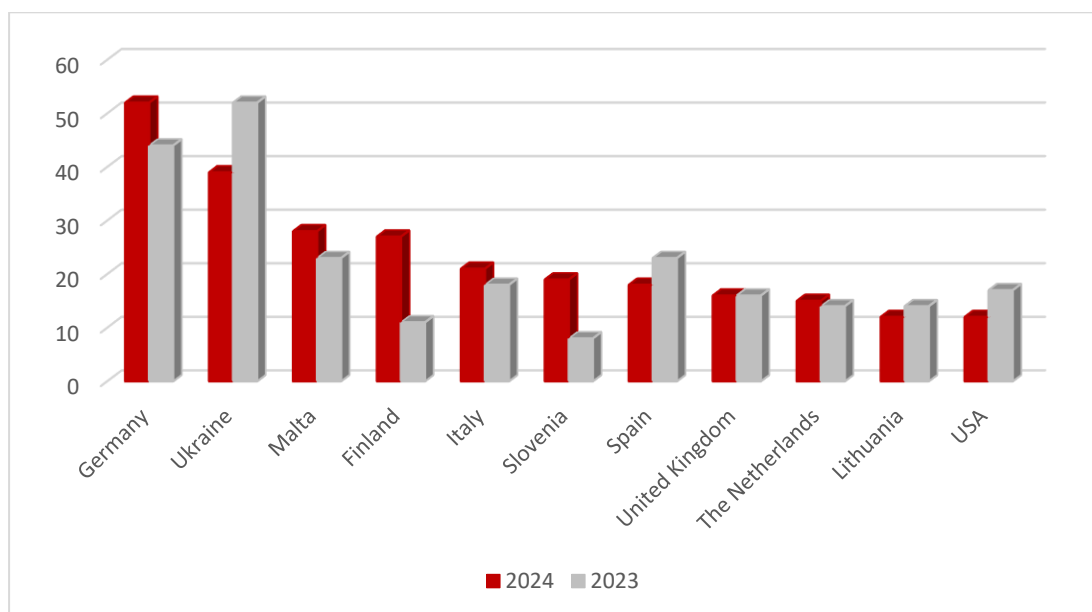
Chart 18. List of the most common predicate offences for money laundering indicated in the requests sent by foreign FIUs in 2024



In 2024, the GIFI also received one request from EUROPOL, which concerned a total of 28 entities. The exchange of information with EUROPOL takes place under Art. 115 of the *AML/CFT Act*.

In 2024, there was a rise in the number of inbound inquiries from Germany compared to the previous year (52 in 2024 compared to 44 in 2023). Moreover, the number of requests from the Slovenian and Finnish Financial Intelligence Units increased significantly. In contrast, the number of requests from the Ukrainian FIU decreased significantly.

Chart 19. Top 10 countries from which foreign FIUs sent the largest numbers of inquiries in 2024 compared to 2023



For the sake of the effective exchange of information between the GIFI and foreign FIUs, the GIFI often facilitates the establishment of cooperation between domestic and foreign law enforcement agencies.

Blocking of funds at the request of a foreign partner

The GIFI received a blocking request from a foreign FIU concerning accounts of citizens of that country held in Polish banks. The reasoning behind the request points to an ongoing investigation in the requesting country into the issuing of falsified documentation and the misrepresentation by a female government official and the financial benefit derived from this practice. During a search of the aforementioned person's home, statements from Polish bank accounts and confirmations of cash payments into Polish accounts were discovered. It was estimated that the aforementioned person had made a financial gain of more than USD 3 million from the practice. The GIFI's analysis showed that besides the official herself, three members of her family, including her husband, also held accounts in Polish banks. These accounts were primarily fed by cash deposits, with the funds then being transferred to three other countries, mainly outside the EU. When asked to document the source of the funds, the civil servant's husband produced, among other things, copies of Cash Declaration Forms submitted at the EU border. The declarations submitted showed that he used the services of "couriers" to transport the cash. Based on this, the GIFI established that the "couriers" named by the civil servant's husband declared EUR 5 million and USD 15 million while entering

Poland over less than one and a half years. In addition, it was also established that another member of the civil servant's family also transported funds across the border, which were then deposited into the account of a Polish company of which he was a co-owner. The funds from the cash deposits were likely invested in the day-to-day operations of the company. This may have been aimed at concealing their criminal origin and generating new, "laundered" revenues. The above is consistent with one method of money laundering, which involves mixing income from legitimate activities with assets from illegal sources.

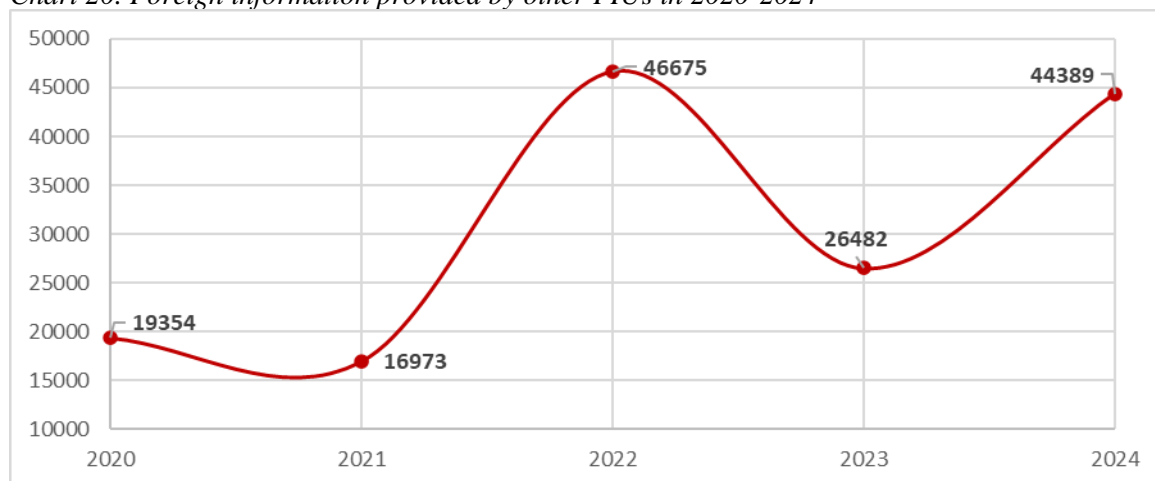
Following its analysis, the GIFI decided to comply with the foreign partner's request and blocked accounts belonging to the suspected corrupt official and her family member.

Besides requests, foreign FIUs provide the GIFI also with foreign information on Polish entities or assets transferred to/from the territory of Poland. This information concerned unusual transactions or possible predicate offences, or was derived from analyses showing a possible connection of the described transactions with money laundering or financing of terrorism. In 2024, the GIFI received a total of 44,389 such communications, 68% more than in 2023, when it received 26,482.

Such information can be divided into the following categories:

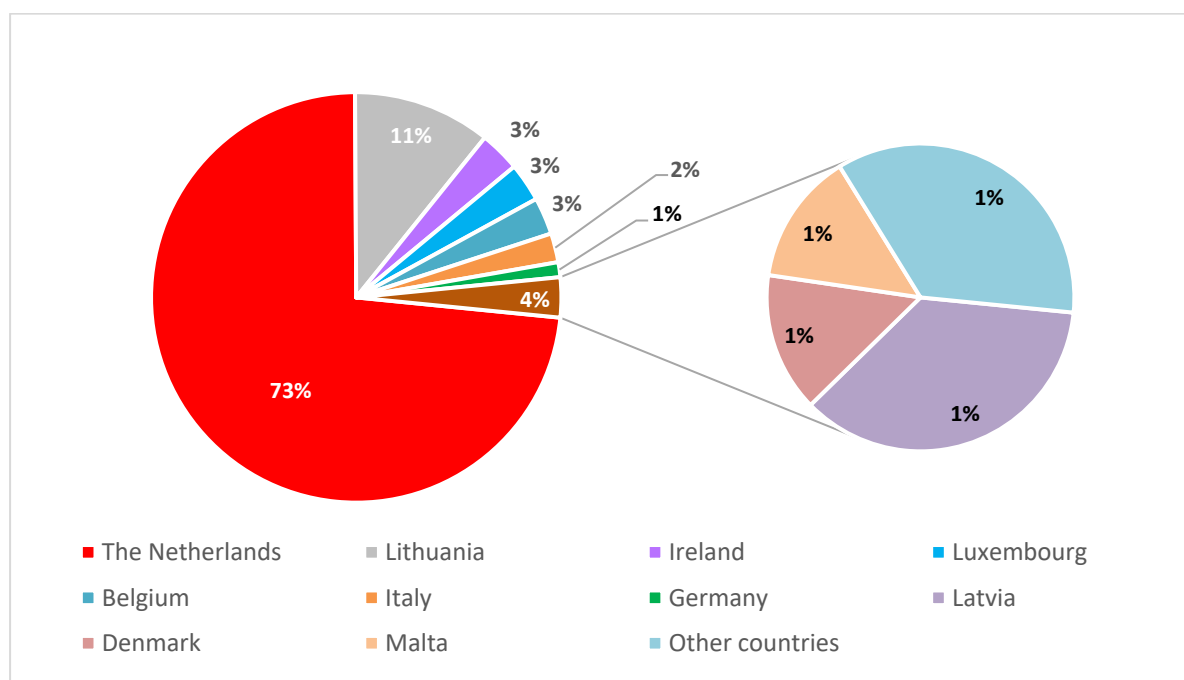
- spontaneous information provided to the GIFI as a result of an operational or strategic analysis performed by another FIU — 499;
- cross-border reports on notifications of suspicious transactions reported by foreign counterparts of obligated institutions in other member states and submitted to the GIFI in accordance with Article 53(1) and (3) of *Directive 2015/849*⁵⁸ — 43,875;
- other information provided by foreign FIUs or institutions and international organisations dealing with counteracting money laundering or financing of terrorism — 15.

Chart 20. Foreign information provided by other FIUs in 2020-2024



⁵⁸ *Directive of the European Parliament and of the Council (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.*

Chart 21. Countries from which foreign FIUs sent the greatest volume of foreign information in 2024

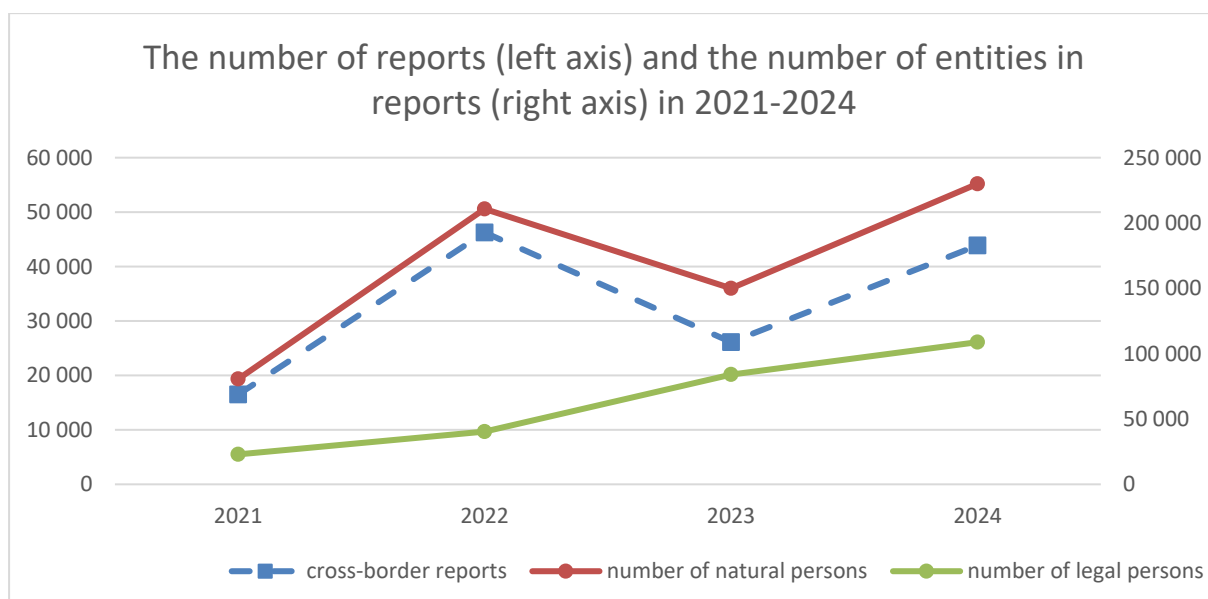


The discussed rise in foreign information was once again due to the number of cross-border reports from the Netherlands, which increased from 19,438 to 32,552. Cross-border reports from the Netherlands, accounting for over 73% of all foreign information, relate to unusual transactions (hence they are called *unusual transaction reports*) that are possibly related to Poland. The information provided usually covers single transactions, which results in numerous received reports. Regarding the remaining partners, there was a significant increase from such countries as Lithuania (an increase of 4,325 reports), Ireland (an increase of 640 reports), Luxembourg (an increase of 583 reports) and Malta (an increase of 99 reports) relative to 2023 figures. In contrast, the analysed period saw a decrease in the number of reports from such partners as Germany (a decrease of 499 reports) or Denmark (a decrease of 146 reports).

Incoming cross-border reports account for 98.8% of all types of foreign information provided by other FIUs. This affects not only the number of reports themselves, but also the amount of information on potentially suspicious entities.

Between 2021 and 2024, the number of *cross-border reports* and *cross-border disseminations* more than doubled, from 16,492 to 43,875. The number of individuals covered by the reports more than doubled as well, while the number of legal entities recorded in the reports increased almost fivefold.

Chart 22. Summary of the number of incoming cross-border reports (left axis) and the number of entities in reports (right axis) in 2021-2024.

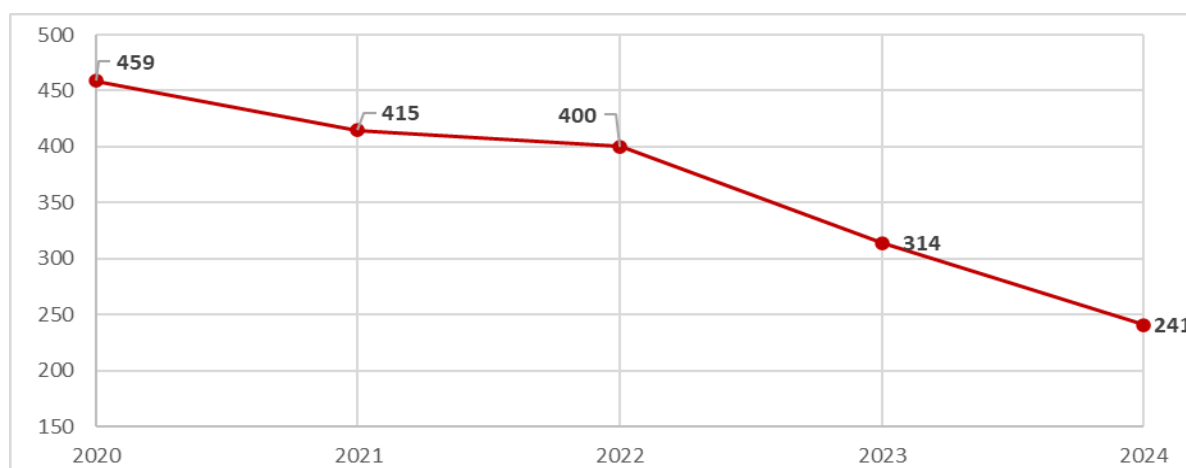


Based on foreign information received from foreign partners, a total of 132 notifications were made in 2024 to cooperating entities,⁵⁹ usually the Police, the National Revenue Administration and the Internal Security Agency. The information received from foreign partners is also taken into account in other notifications and notifications to cooperating units, developed on the basis of the results of the conducted analytical proceedings.

Requests and information provided by the GIFI to its foreign partners

In 2024, the GIFI sent a total of 241 requests for information, of which the majority (62% of requests) were addressed to EU member states.

Chart 23. Inquiries sent by the GIFI to foreign FIUs in 2020-2024

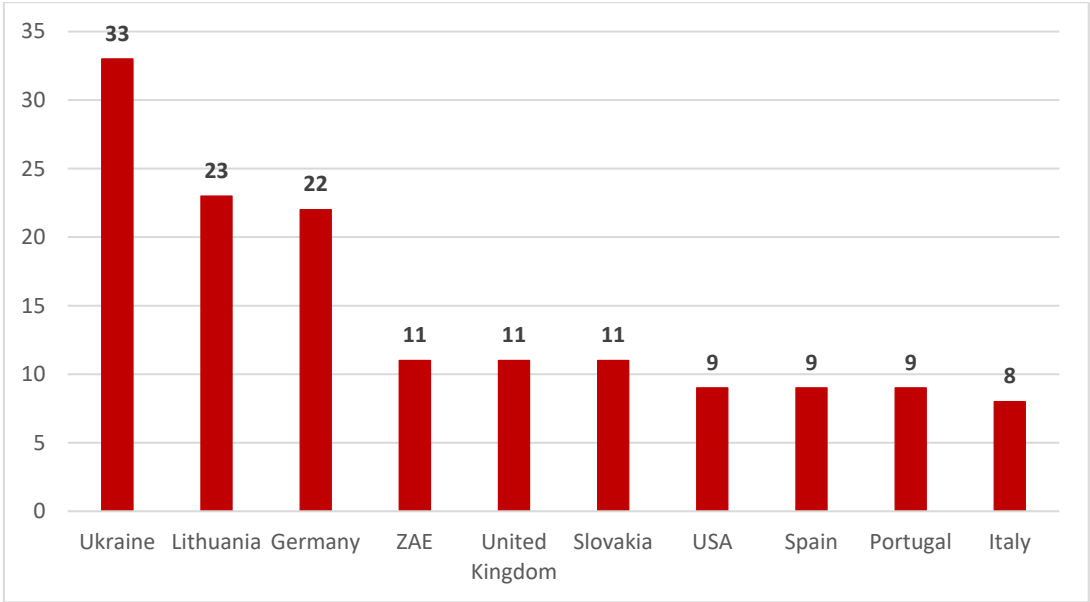


In connection with the conducted analytical cases, the GIFI cooperated most often with the FIUs from Ukraine, Germany and Lithuania (similar to 2023). Information obtained from abroad is used primarily to verify whether entities involved in transactions that obligated institutions and cooperating units find suspicious are known to the FIU in connection with suspected money laundering, financing of terrorism or involvement in other criminal activities.

⁵⁹ Statistics on notifications to cooperating entities are included in the statistics presented in Chapter 4.1.1.

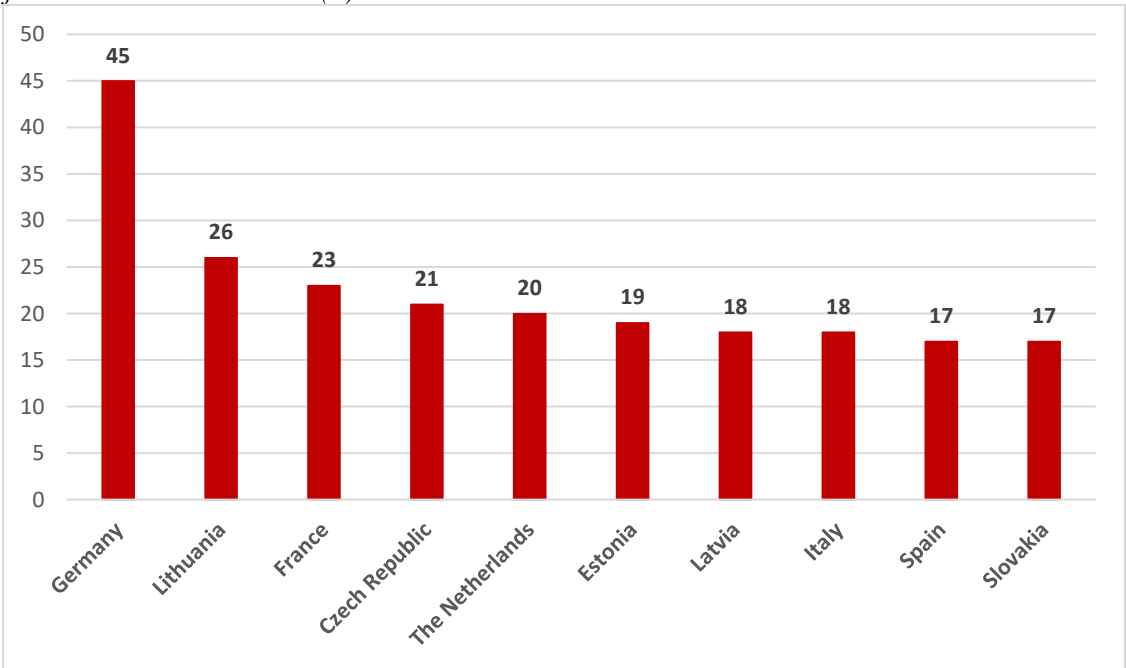
The GIFI also receives data and information on financial flows, which makes it possible to determine the source of funds transferred to Poland or the further path of cash flows.

Chart 24. Top 10 countries – foreign FIUs to which the GIFI sent the largest numbers of inquiries in 2024



In 2024, the GIFI, acting under Article 112(3) of the [AML/CFT Act](#), drew up a total of 354 reports on notifications relating to other EU member states for foreign Financial Intelligence Units.

Chart 25. Top 10 countries – foreign FIUs for which the GIFI drew up the largest numbers of notifications under Article 112(3) in 2024



Apart from cross-border reports, 25 spontaneous notification containing the results of the GIFI's analytical investigations were also transmitted to foreign partners. The greatest number of them (8) were provided to the Ukrainian FIU.

7.10. OTHER INTERNATIONAL INITIATIVES

7.10.1. THE PROJECT "STRENGTHENING THE RISK ASSESSMENT MECHANISMS AND THE STRATEGIC ANALYSIS FUNCTION OF THE POLISH FINANCIAL INTELLIGENCE UNIT"

In 2024, work continued on the TSI project "Strengthening the Risk Assessment Mechanisms and the AML/CFT Strategic Analysis Function of the Polish Financial Intelligence Unit", underway since the first half of 2022, with the financial support of the Council of Europe and the European Commission (DG REFORM). The aim of the project was to improve the national *AML/CFT* framework so that it complies with FATF standards and EU regulations.

The project as a whole envisaged the delivery of 7 outputs.

- I. **Output 1.** "Revised methodology for future national ML/FT risk assessments".
- II. **Output 2.** "Mapping data available for the national ML/FT risk assessment to identify gaps and provide recommendations to address identified deficiencies".
- III. **Output 3.** "Updated national ML/FT risk assessment" — fully achieved in the previous years of the project (2022–2023).

Among the additional results achieved in 2024, the following activities were carried out:

As part of **Output 4.** "Sectoral ML/FT risk assessments to complement the KAS, among others, in the area of virtual assets (VA) and virtual asset service providers (VASP)":

- On 28-30 August 2024, a training course on operational and strategic analysis of cases related to cryptocurrency trading was held in Warsaw for representatives of the FIU and cooperating units.
 - Between April and September 2024, Council of Europe experts, together with FIU staff, developed a sectoral analysis of VASPs.
 - On 11 September 2024, the Council of Europe presented a revised draft document entitled "Review of the cryptocurrency market in Poland. The Impact of the MiCA Regulation on the Operation of the VASP Sector in Poland, Including the Mitigation of ML/TF risk".
- IV. As part of **Output 5.** "Guide on strengthening the strategic analysis function in the Polish FIU":
- On 20–21 March 2024, the Council of Europe and DG REFORM organised an international conference entitled "Enhancing the Strategic Analysis function of the FIUs – experiences, needs and challenges".
 - On 17–20 September 2024, a strategic analysis training course was held in Warsaw for FIU staff. The training was divided into two parts. The first, dedicated to FIU staff, was the "Workshop on the strategic analysis manual for the Polish FIU" while the second — "Strategic Analysis Training" — was prepared jointly with Egmont Group and dedicated to both FIUs and cooperating units.
- V. As part of **Output 6.** "Advice on improving mechanisms for information exchange between the FIU and other competent authorities, including law enforcement agencies

(LEAs), as well as on the implementation of electronic suspicious activity reporting (eSAR) within the national financial regulation and supervision system”:

- On 19 March 2024, two bilateral meetings were held in Warsaw between representatives of the Polish FIU and representatives of FIUs from Latvia and Luxembourg. They served to exchange experience in the use of IT tools in the acceptance and processing of eSAR reports.
 - 21 March 2024 saw the organisation of a workshop entitled "Implementation of electronic suspicious activity reporting (eSAR) in Poland as part of the national financial regulation and supervision system".
 - Two study visits of Polish FIU representatives related to the use of IT tools in receiving and processing SAR reports were held. The meetings took place on 5–6 September 2024 in Vienna and 13 September 2024 in Riga.
- VI. As part of **Output 7**. “Strengthening the capacities of the FIU through workshops aimed to exchange experiences with the FIUs of other Member States”:
- On 24-25 September 2024, training on the use of open source intelligence (OSINT) for operational and strategic analysis was conducted in Warsaw.

In addition, several meetings of the Project Advisory Group (PAG) were held during the year, attended by representatives of the GIF, cooperating units (Ministry of Justice, National Prosecutor's Office, Internal Security Agency, Office of the Polish Financial Supervision Authority, National Police Headquarters, Central Investigation Bureau of the Police, The Border Guard and the National Bank of Poland) and DG REFORM and the Council of Europe. The meetings were used to monitor the progress of the project and agree on the sequence of further actions.

The project also produced 8 technical documents containing knowledge and a set of best practices in the thematic areas covered by the project: "Strategic Analysis Handbook for the Polish Financial Intelligence Unit", "Review of methodologies for national money laundering and terrorist financing risks with recommendations", "Review of data and data sources used by Poland in the development of the National Risk Assessment with recommendations", "Implementation of Electronic Suspicious Activity Reporting (eSAR) in Poland within the national system of financial regulation and supervision", "Review of the current procedures and framework for information exchange between the Polish Financial Intelligence Unit and other competent ML/TF authorities", "Virtual Asset Service Providers (VASPs) and international examples of their ML/TF abuse in relation to different sectors and other obligated institutions", "Research on the regulation of VASPs and international practices in conducting sectoral risk assessment of VASPs", as well as "Review of the Polish institutional and legal framework related to the performance of the strategic analysis function of the Polish Financial Intelligence Unit".

The work on the project was completed on 30 September 2024.

7.10.2. WORKSHOP FOR UKRAINIAN ADMINISTRATION REPRESENTATIVES CO-HOSTED WITH THE OSCE

On 5–8 February 2024, the GIFI (in cooperation with the OSCE) organised a workshop on the most common money laundering risks, supervisory issues in the VASP sector and current legislative issues related to this sector. The meeting was attended by Ukrainian administration representatives working in the field of anti-money laundering and counter-terrorist financing. The workshop was conducted by OSCE international experts, representatives of supervisory authorities and financial institutions. The event organised by the OSCE and the GIFI in February 2024 was followed by workshops for Ukrainian partners on 18–20 June. The workshop addressed the risks of money laundering using crypto-assets and the new regulations for the Virtual Asset Service Provider sector, including issues of supervision of the sector. The workshop was led by international OSCE experts, representatives of supervisory authorities and financial institutions, and apart from the Ukrainian side (representatives of the National Bank of Ukraine, the National Securities and Exchange Commission of Ukraine, the State Financial Monitoring Service of Ukraine and the Ministry of Digital Transformation of Ukraine), it was also attended by representatives of Polish institutions involved in the issues of combating money laundering using crypto-assets. Approximately 40 people attended the meeting. The event took place at the Ministry of Finance, with some participants joining remotely.

In July 2024, the GIFI signed a letter of intent in which it emphasises its readiness to support workshops and training organised by the OSCE and confirms that cooperation with the OSCE is in line with the GIFI's broader objectives in the fight against financial crime, particularly in the area of virtual assets and cryptocurrencies.

7.10.3. FIU REGIONAL WORKSHOPS UNDER THE POLISH PRESIDENCY OF THE V4

On 28-29 November 2024, Regional Workshops for Financial Intelligence Units were held in Warsaw. The event was hosted by the GIFI and the participants were representatives of Financial Intelligence Units from the Visegrád Group (V4), i.e. Czech Republic, Poland, Slovakia and Hungary. As is customary, one country from outside the V4 Group was invited to attend the meeting; this time it was Germany. The meeting was primarily devoted to the exchange of views and experiences and to gathering information on best practices in counteracting money laundering and financing of terrorism in Central European countries.

7.10.4. STUDY VISITS

STUDY VISIT OF A DELEGATION FROM UKRAINE

A study visit by a delegation from the Ukrainian Financial Intelligence Unit took place on 11-12 March 2024, dedicated to issues related to IT tools used at FI for data analysis. Representatives of the Ukrainian Financial Intelligence Unit had the opportunity to learn about DataWalk software, as well as the possibilities and methods of implementing the goAML system in a financial intelligence unit. The visit was also an opportunity to exchange experiences in the field of data analysis conducted in Financial Intelligence Units.

VISIT OF A TURKISH REPRESENTATIVE

On 25 July 2024, a meeting with a representative of the Turkish Gendarmerie was held at the Ministry of Finance. The meeting focused on the GIFI activities in the area of disclosure and prevention of money laundering and financing of terrorism. Aside from the GIFI representatives, the meeting was also attended by employees of the Mazowieckie Region Customs and Tax Office in Warsaw. The issues presented included legislative solutions applied in Poland, as well as tools and measures taken to suspend transactions and block accounts. The meeting was an excellent opportunity to exchange knowledge and experience, as well as to discuss possibilities for closer cooperation in the global fight against money laundering and the financing of terrorism.

STUDY VISIT OF A DELEGATION FROM NIGERIA

A study visit by a delegation from the Nigerian Financial Intelligence Unit, led by its head, Ms Hafsat Bakari, took place on 5–6 September 2024. The purpose of the visit was to showcase Poland's expertise in activities related to crypto assets and the register of beneficial owners. The Nigerian representatives presented their experience with improving the efficiency of case system management using artificial intelligence and machine learning.

7.10.5. OTHER INITIATIVES

WORKSHOP ON INTERNATIONAL AND EU STANDARDS FOR INVESTIGATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM, ORGANISED JOINTLY WITH THE EU AML/CFT GLOBAL FACILITY

The workshop was held on 3–4 June 2024 as another initiative to support Ukraine in its activities in the area of combating money laundering and the financing of terrorism.

The speakers at the meeting included foreign experts from the EU *AML/CFT* Global Facility, a key European Union project in the fight against money laundering and the financing of terrorism.

The meeting presented the international legal framework facilitating financial investigations, good practices in combating the financing of terrorism, the role of law enforcement agencies and Financial Intelligence Units in investigations into money laundering and financing of terrorism, as well as case studies.

The meeting was attended by approximately 30 participants representing Polish and Ukrainian administration, including representatives of the GIFI, the Ministry of Finance's Department for Combating Economic Crime, the Ukrainian Financial Intelligence Unit (SFMS) and the National Anti-Corruption Bureau of Ukraine (NABU).

WORKSHOP ON COOPERATION WITH HIS MAJESTY'S REVENUE AND CUSTOMS (HMRC), ORGANISED JOINTLY WITH THE KAS

On the initiative of the HMRC PCU, the UK treasury's unit for high-priority criminals, a joint GIFI–KAS workshop was held on 4 June 2024 at the Ministry of Finance to gain a better understanding of how economic crime systems work in Poland and the UK and how the organised crime units of the Polish and UK tax administrations operate. During the meeting,

opportunities for mutual exchange of information and possible joint activities were also discussed. The meeting was attended by representatives of the GIFI, the Department for Combating Economic Crime, one customs and tax chamber, as well as HMRC and the British Embassy in Warsaw.

"ARTICLE 75 LEADERS' WORKSHOP" CO-ORGANISED WITH THE POLISH BANK ASSOCIATION

On 9 December 2024, the GIFI co-organised a workshop at the Bankers' Club on the implementation and application of Article 75 of *Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. The workshop was organised as part of the Future of Financial Intelligence Sharing (FFIS) programme by RUSI Centre for Financial Security and the Polish Bank Association (ZBP).

The event aimed to present changes in EU law on information sharing partnerships and international good practices in this area, and to encourage the development of own plans and standards for the implementation of Article 75 of the above Regulation.

The workshop was held as part of a research project involving the organisation of a series of meetings in EU member states to help representatives of the public and private sectors discuss any obligations and issues arising from Article 75 of the Regulation, and to support them in developing partnerships tailored to their priorities and legal regimes.

7.10.6. AEOI REVIEW⁶⁰

At the invitation of the Department of International Cooperation of the National Revenue Administration, which coordinated the review of Poland's compliance with the CRS (Common Reporting Standard) by financial institutions, the GIFI representatives participated in a visit by OECD Global Forum evaluators, which took place on 4–6 June 2024 at the Ministry of Finance in Warsaw. The visit aimed to gain a better understanding of the implementation of CRS requirements in Poland, as well as the characteristics of the financial institution market, in particular the basic requirements for national reporting of information by financial institutions and the control of this process by the Polish administration. The GIFI representatives answered questions concerning such things as the functioning of financial institutions which are obligated institutions within the meaning of the provisions on counteracting money laundering and the financing of terrorism, from the perspective of the control exercised over them by the GIFI. The questions addressed to the GIFI representatives also covered certain aspects of the National Assessment of the Risk of Money Laundering and Financing of Terrorism, as well as the GIFI's cooperation with the National Revenue Administration. The GIFI also provided comments on the draft report prepared following the on-site visit. The GIFI participated in the second round of Poland's evaluation review in terms of assessing the Exchange of Information on Request (EOIR). Activities in this area are monitored as part of the member states' peer review system, implemented by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes.

⁶⁰ Automatic Exchange of Information.

The second round of OECD peer reviews included enhanced standards for the availability of beneficial owner information (as defined in the FATF Recommendations), including access to it by tax authorities. Accordingly, the review covered the issues of beneficial owners as well as the register of beneficial owners, among other things.

The GIFI representatives participated in activities coordinated by the Ministry of Finance: they prepared answers to the questionnaire, participated in a meeting with OECD experts, answered additional questions and provided opinions on the draft *Peer Review Report on the Exchange of Information on Request Poland 2023 (Second Round, Combined Review)* published on the OECD website following its approval on 3 November 2024.

Poland was assessed in the report as "*largely compliant*" with the OECD standards for the exchange of tax information on request.

The next step in the review will be to implement the OECD report's recommendations, including those relating to the availability of accounting and banking information, ownership and identity information, access to information requested under information exchange agreements and the rights and safeguards available to taxpayers and third parties.

7.10.7. CHOOSING THE SEAT AND APPOINTING THE CHAIR OF THE AMLA

In 2024, work on the selection of the seat and chair of the AMLA came to an end. The Minister of Finance and the GIFI were actively involved in this process. Meetings and discussions were held with representatives of countries applying to host the AMLA headquarters. On 22 February 2024, Frankfurt am Main was chosen as the seat of the AMLA.

In 2024, steps were also taken to elect the chair of the AMLA. The European Commission selected three candidates from the open call for applications for the shortlist: representatives from Germany, Italy and the Netherlands. On 18 December 2024, the European Parliament recommended the candidacy of Ms Bruna Szego, representative of Italy.

7.11. INTERNATIONAL COOPERATION IN THE AREA OF AML/CFT SUPERVISION AND CONTROL

7.11.1 COOPERATION WITH THE EUROPEAN BANKING AUTHORITY (EBA)

Since 2020, pursuant to Article 9a(7) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council establishing a European Supervisory Authority (European Banking Supervision Authority — "EBA"), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12, as amended), hereinafter referred to as Regulation 1093/2010, a Standing Committee on Anti Money Laundering and Countering Terrorist Financing ("AMLSC") has been operating at the EBA.⁶¹ Its main purpose

⁶¹ In accordance with Regulation 1093/2010, the AMLSC is composed of high-level representatives of authorities and bodies from all member states competent to ensure the compliance of financial sector entities with Regulation 2015/847 and Directive 2015/849, representatives of the EBA, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority. Further, the Commission, the European Systemic Risk Board and the European Banking Authority each appoint a high-level representative to participate in the meetings of the Committee as observers.

is to coordinate measures to prevent and combat the use of the financial system for money laundering or the financing of terrorism. The AMLSC also prepares, in accordance with the provisions of *Directive 2015/849 and 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* (hereinafter referred to as Regulation 2015/847, OJ L 141, 5.06.2010, pp. 1-18), all draft decisions adopted in this respect by the EBA.

In 2024, representatives of the GIFI actively participated in the meetings of the AMLSC and together with representatives of the Office of the Polish Financial Supervision Authority (UKNF) and the National Bank of Poland (NBP) represented Poland in the Committee. Both authorities cooperate with each other on an ongoing basis as part of the analysis of materials prepared for the meetings. In 2024, four meetings of the AMLSC were held. During the meetings, topics related to, among others, work carried out by the Committee, including the preparation of draft EBA guidelines, were discussed. The outputs of the work of the competent national authorities in the AML/CFT area, within the AMLSC, include the publications of EBA AML/CFT guidelines addressed to obligated institutions and competent authorities. Discussions on current AML/CFT events (e.g. risks related to cryptocurrencies, vIBAN⁶² and international sanctions) were also undertaken at the meetings.

Moreover, EBA reports and opinions prepared by its working groups (which may include representatives of the European Supervisory Authorities (ESAs), as well as experts from competent national authorities) were also put to the vote at the meetings. In 2024, the EBA also maintained ongoing contact with representatives of EU member states to exchange information and collect additional information from competent national bodies, including by sending questionnaires (e.g. regarding the regulation of AML/CFT issues in national law — such data and information is meant to help in the implementation of tasks imposed on the EBA) to representatives of the above-mentioned bodies.

AML/CFT Colleges

In 2024, Poland continued cooperation with other competent national authorities in the area of AML/CFT as part of *Joint Guidelines JC/GL/2019/81 of 16 December 2019 on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions* (The AML/CFT Colleges Guidelines) published by the EBA.⁶³ In 2024, the GIFI representatives participated in eight meetings of the AML/CFT colleges, in which the GIFI's participation was substantiated by its role as an FIU and that of the authority controlling obligated institutions. During the meetings, topics related to AML/CFT supervision of entities to which the colleges relate were discussed and information was exchanged between the competent authorities being members of the AML/CFT college.

Provision of information on administrative sanctions by the GIFI to the EBA

Pursuant to Article 60 of *Directive 2015/849*, member states "shall ensure that a decision imposing an administrative sanction or measure for breach of the national provisions transposing this Directive against which there is no appeal shall be published by the competent

⁶²Virtual International Bank Account Number.

⁶³ <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/jc-guidelines-on-cooperation-and-information-exchange-for-aml/cft-supervision-purposes>

authorities on their official website immediately after the person sanctioned is informed of that decision".

Pursuant to Article 62(1) of *Directive (EU) 2015/849*, Member States shall ensure that their competent authorities inform the European Supervisory Authorities (i.e. EBA, ESMA, EIOPA) of all administrative sanctions and measures imposed in accordance with Article 58 and Article 59 of *Directive 2015/849* on credit or financial institutions, including any appeal in relation thereto and the outcome thereof.

Pursuant to Article 152(7) of the *AML/CFT Act*, information on imposing an administrative sanction on obligated institutions shall be submitted to the European Supervision Authorities. Under the above regulations, the GIFI shall provide, on an ongoing basis, information on administrative sanctions via the eGATE and EuReCa platforms operated by the EBA.

In 2024, the GIFI submitted the following number of reports on administrative sanctions imposed by the GIFI, the Minister of Finance, the President of the National Bank of Poland and the Polish Financial Supervision Authority: 24 via eGATE. No reports with information on administrative sanctions imposed were submitted via the EuReCA platform in 2024.

7.11.2 COOPERATION WITH COMPETENT SUPERVISORY AUTHORITIES IN PARTICULAR COUNTRIES

In 2024, pursuant to Article 50a of *Directive 2018/843*, the GIFI made one request for AML/CFT information to the EU Member State authority competent for supervision in the area of counteracting money laundering and financing of terrorism, acting pursuant to Article 116 of the *AML/CFT Act*.

In 2024, no requests were made to the GIFI by foreign FIUs under Article 50a of *Directive 2018/843* to provide information on the monitoring and analysis of money laundering and financing of terrorism.

In 2024, the GIFI responded to a request by a national AML/CFT authority of an EU member state by stating that it had no information on the matter raised in the request.

Acting pursuant to Article 115a of the *AML/CFT Act*, the GIFI made eleven requests, in cooperation with the competent supervisory authorities of EU member states, concerning six institutions obliged to report suspicious transactions.

8. APPLICATION OF SPECIFIC RESTRICTIVE MEASURES

Pursuant to the *AML/CFT Act*, obligated institutions are required to apply specific financial restrictive measures with respect to persons and entities entered on the sanctions lists published on the GIFI's website.

In 2024, the GIFI informed obligated institutions and cooperating units about the rules for applying specific restrictive measures as part of the training series organised in connection with the implementation of activities provided for in the *AML/CFT Strategy*.

Obligated institutions that registered for the GIFI's sanctions newsletter received information on current changes to the sanctions lists. The GIFI sent out seven newsletters throughout 2024.

In 2024, the Financial Security Committee assessed the circumstances justifying the continued need for specific restrictive measures against two persons included in September 2023 on the list referred to in Article 120(1)(2) of the *AML/CFT Act* (the so-called national sanctions list) who are suspected of having links with terrorism or its financing.⁶⁴ The Committee did not confirm that no such circumstances existed, and the entries were therefore maintained. Obligated institutions apply specific restrictive measures with regard to persons placed on the list, which consist in freezing assets and refusing to make them available, and in the event of application of these measures, they immediately notify the GIFI accordingly.

The GIFI did not receive any notification of freezing assets of entities included in the sanctions lists related to counteracting the financing of terrorism, or refusal to make assets available to such entities.

The GIFI monitored the obligated institutions' compliance with the restrictive measures set out in *Regulation 765/2006*, *Regulation 269/2014*, *Regulation 833/2014* and in the *Act of 13 April 2022 on Special Measures to Counteract the Support of Aggression Against Ukraine and to Protect National Security*.

The GIFI participated in the work on the draft uniform sanctions act and the draft amendments to the *Act of 13 April 2022 on Special Measures to Counteract the Support of Aggression Against Ukraine and to Protect National Security*. Work has also commenced on amendments to the *AML/CFT Act* to include regulations on sanctions aimed at countering the proliferation of weapons of mass destruction and their financing, applicable to persons and entities with ties to Iran or North Korea. The pending amendments to the legislation are aimed at tidying up the legislative framework for the application of sanctions in Poland and ensuring consistency in the regulation of all issues related to their enforcement.

In 2024, the GIFI representatives participated as listeners in meetings of the Freeze and Seize Task Force and the associated Asset Freezes and Reporting Subgroup within the Expert Group on EU Restrictive Measures and Extraterritoriality, established in connection with the war in Ukraine. The Freeze and Seize Task Force meets regularly to ensure better coordination among Member States in the enforcement of EU sanctions against Russian and Belarusian individuals and entities and to strengthen cooperation between the European Union and its international partners, including the US and Ukraine. The aim of the Asset Freezes and Reporting Subgroup is to examine how the implementation of EU restrictive measures for asset freezing and

⁶⁴<https://www.gov.pl/web/finanse/lista-osob-i-podmiotow-wobec-ktorych-stosuje-sie-szczegolne-srodkio-graniczajace-na-podstawie-art-118-ustawy-z-dnia-1-marca-2018-r-o-przeciwdzialaniu-praniu-pieniedzy-i-finansowaniu-terroryzmu>

reporting on freezes can be improved, in particular in the context of the sanctions for violations of the territorial integrity of Ukraine (Council Regulation (EU) No 269/2014).

9. FINANCIAL SECURITY COMMITTEE

Three meetings of the Financial Security Committee ("Committee") were held in 2024.

During the meetings, Committee members presented information on and discussed such things as:

- activities under the "Strategy for Counteracting Money Laundering and Financing of Terrorism";
- activities carried out as part of the AML/CFT Strategy provided for within its particular priorities;
- periodic assessment of the circumstances justifying the continued need to apply specific restrictive measures to individuals and entities on the GIFI sanctions list;
- the concept of information exchange between the FIU and cooperating units (particularly law enforcement agencies) by means of an ICT system;
- the work of the Working Group for cooperation between representatives of the public, private and public-private sectors;
- the creation within the Committee of a working group on identifying and countering threats in the crypto asset market;
- amending the Committee's Rules of Procedure to strengthen the expert nature of the working groups set up at the Committee and to increase the Committee's operational capacity;
- progress in implementing the recommendations of the MONEYVAL experts, included in the report on the evaluation of the Polish AML/CFT system.

The Committee worked on agreeing upon actions to be included in the new "Strategy for Counteracting Money Laundering and Financing of Terrorism". The Strategy will apply from 2025 to 2027. In designing the themes for the actions, the coordinator and the units implementing the actions were identified. The members of the Committee provided written opinions on the draft of the new AML/CFT Strategy, and the comments made were discussed during the Committee meetings.

Pursuant to Articles 124 and 125 of the *AML/CFT Act*, the Committee assessed the circumstances justifying the continued application of specific restrictive measures against persons or entities included on the list referred to in Article 120(1) by the GIFI's decision of 22 September 2023.

The Committee members did not identify any circumstances that would justify removal from the list, thereby confirming the need to maintain the specific restrictive measures against the persons included in the list.

In 2024, a meeting was also held of the Working Group for cooperation among public, private and public-private sector, operating under the auspices of FSC and teams established under the Group in 2024 continued to operate, including the Working Group for the Banking Sector, the Working Group for Payment Institutions, the Working Group for the Legal Professions, as well

as the Working Group for Virtual Asset Service Providers. The cooperation with representatives of the private sector within the above working groups made it possible to address issues and effectively resolve problems considered to be priorities from the perspective of cooperation between the GIFI and a specific category of obligated institutions represented in the group.

Efforts to establish a Working Group for identifying and counteracting threats in the crypto asset market were initiated by the Central Bureau of Investigation (Central Investigation Bureau of the Police). This work included preparing and consulting on a draft resolution on the establishment of the Group. At the same time, the Committee took steps to remove restrictions in its Rules of Procedure on appointing people from outside the Committee to working groups and letting them lead these groups. In this regard, draft amendments to the Rules of Procedure of the Committee were prepared. The adoption of these amendments as well as the adoption of a resolution on the establishment of the Working Group is planned for 2025.

10. WORK ON UPDATING THE STRATEGY FOR COUNTERACTING MONEY LAUNDERING AND FINANCING OF TERRORISM

In late 2023, the GIFI worked with the Financial Security Committee, cooperating entities and obligated institutions to prepare the second edition of the National Assessment of the Risk of Money Laundering and Financing of Terrorism ("NRA"). The document was signed (accepted) on 27 November 2023 by the minister competent for public finance and published in the Public Information Bulletin on the website of the office supporting the minister competent for public finance.

Pursuant to Article 31(2) of the *AML/CFT Act*, in the event of a change in the NRA or where required by the implementation of the European Commission recommendations referred to in Article 6(4) of Directive 2015/849, the GIFI shall prepare a draft update of the strategy for counteracting money laundering and financing of terrorism ("strategy"). Work on the update of the strategy commenced in early 2024. A key element of these measures was the letter sent by the GIFI in March 2024 to FSC members requesting comments, suggestions and feedback on the provisions and measures implemented under the strategy adopted by *Council of Ministers Resolution No. 50 of 2021 on the adoption of a strategy for counteracting money laundering and financing of terrorism*, as well as proposals for measures to be included in the update of this document. Cooperation with FSC members resulted from the fact that the Strategy is not only aimed at planning the activities of the GIFI as the coordinator of the system for counteracting money laundering and financing of terrorism, but above all at properly highlighting and mitigating the most important risks identified in the NRA. The inclusion of the opinions and needs of institutions participating in the national system for counteracting money laundering and financing of terrorism is crucial for the creation of a more effective and comprehensive strategy. Furthermore, a new important factor affecting the AML/CFT system emerged during the strategy's preparation — the adoption by the European Union of a package of regulations to strengthen the tools for combating money laundering and the financing of terrorism (the so-called AML Package). The new EU regulations will have a significant impact on the principles of functioning of the GIFI, control and supervisory bodies of the AML/CFT system and their role in the system. The EU's adoption of the AML Package requires that its provisions be taken into account in the strategy to ensure consistency and effectiveness of operations within the Polish AML/CFT system.

An FSC meeting was held on 4 July 2024, at which the GIFI summarised the activities carried out under the first strategy, which were included in the draft "Report on the implementation of the strategy for counteracting money laundering and financing of terrorism". Comments on the implementation of the first strategy had to be taken into account in the proposals for measures to update the new AML/CFT strategy. At the next FSC meeting on 10 September 2024, a summary of comments and proposals submitted by FSC members (including the GIFI) on the new AML/CFT strategy was discussed, together with a proposal for more than twenty actions based on those comments and proposals. On 17 September 2024, the GIFI again asked FSC members to comment on or make potential changes to the list of proposals submitted at the FSC meeting on 10 September 2024 and to provide additional suggestions for the draft new AML/CFT strategy. In response, comments, proposals for action and recommendations

concerning the development of the national system for counteracting money laundering and financing of terrorism were submitted. The GIFI analysed the comments and proposals submitted, which constituted an important element in the development of the strategy update. To ensure consistency and effectiveness of measures proposed by different institutions and to balance differences in risk assessment, priorities or proposed solutions, the GIFI has repeatedly provided a forum for discussion and dispute resolution through bilateral or multilateral working meetings of AML/CFT system participants. Common positions were developed in relation to proposed actions, taking into account the diverse views and perspectives of system participants. The resulting draft strategy was presented at the FSC meeting held on 19 December 2024. Work on the draft strategy is currently continuing.

.

11. LEGISLATIVE ACTIVITY

In 2024, the legislative activity of the GIFI concerned, in particular, communication with obligated institutions and cooperating units, and consisted in ongoing sharing of AML/CFT knowledge in the Public Information Bulletin on the website of the office supporting the minister competent for public finance, in the form of the GIFI's communications.

In addition, in 2024, representatives of the Department of Financial Information participated in the work of the EU working group on the AML/CFT regulatory package.

The GIFI was also responsible for providing ongoing opinions on draft legislation within its remit.

Further, work began in 2024 on amending the provisions on counteracting money laundering and financing of terrorism. On 4 November 2024, a *draft act* amending the *Act on counteracting money laundering and financing of terrorism* was entered into the List of Legislative and Programme Work of the Council of Ministers under No. UC75.

The draft provides, among other things, for supplementing the provisions of the *AML/CFT Act* with regulations concerning restrictive measures used to counteract the proliferation of weapons of mass destruction as well as the financing of their proliferation. Moreover, it contains provisions to ensure that the provisions of the aforementioned Act are consistent with those 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* in its current wording. In addition, the draft aims to bring the *AML/CFT Act* into line with specific recommendations contained in MONEYVAL's 5th round evaluation report on Poland regarding anti-money laundering and counter-terrorist financing measures.

In 2024, the Department of Financial Information also participated in legislative work related to many other draft normative acts falling within the remit of the financial intelligence unit. Among the most important of these is the crypto-assets market bill (UC2).