ANNEX 2 – ANALYSIS OF MONEY LAUNDERING AND TERRORISM FINANCING RISK BY SECTORS

AREAS

Area	Money laundering			Terrorism financing		
	Averaged vulnerability	Averaged threat	Estimated level of risk	Averaged vulnerability	Averaged threat	Estimated level of risk[1]
1. Area – banking	2.75	2.75	2.65	2.75	3.0	2.31
2. Area – payment services (offered by entities other than banks)	3.0	2.33	2.64	3.33	3.67	2.68
3. Area – insurances	2.0	2.0	2.20	3.0	1.0	1.92
4. Area – other financial institutions	2.0	2.2	2.25	2.0	1.0	1.56
5. Area – foreign currency exchange	2.33	3.33	2.64	2.0	2.0	1.80
6. Area – virtual currencies	3.0	3.0	2.80	3.0	3.0	2.40
7. Area - telecommunications services linked with mobile payments	4.0	2.0	2.92	4.0	1.0	2.28
8. Area – physical cross-border	3.5	3.5	3.10	.0	3.5	2.88

[1]The estimated level of risk for each sector is calculated in accordance with the rules for national risk assessment set out in Annex 1. For each area, the averaged level of threat and vulnerability of money laundering and, separately, of terrorism financing was estimated. It was followed by the estimation of the level of probability separately for money laundering and terrorism financing in each sector (using the formula: Pprs = 40% *Zps + 60%*Pps, where Pprs – Level of probability, Zps – Level of threat, Pps – Level of vulnerability. In the next stage, the risk of money laundering and the risk of terrorism financing was calculated for each sector separately (according to the formula: Rps = 60% *Pprs + 40% *Krp, where: Rps – Level of risk, Pprs – Level of probability, Krp – Level of ML consequences fo the purposes of "inherent risk" assessment"). The adopted assumptions on the level of consequences in the area of money laundering in the area of inherent risk were estimated at 2.5, while the assumptions on the level of consequences in the area of terrorism financing in the scope of inhereint risk were estimated at 1.5.

transportation of illicit proceeds						
9. Area – gambling	2.0	2.75	2.38	2.0	1.0	1.56
10. Area – non-profit organisations	3.0	3.0	2.80	3.0	2.0	2.16
11. Area – crowdfunding	4.0	2.0	2.92	4.0	2.0	2.52
12. Area - trade in high-value goods	3.0	2.5	2.68	3.0	1.5	2.04
13. Area – business activity (in general)	2.5	4.0	2.86	2.0	2.0	1.80
14. Area - real estates	2.0	3.0	2.44	2.0	3.0	2.04

1. Area – banking

Sector description - is contained in sub-chapter 2.1.2. of NRA "Financial market sectors" and in sub-chapter 7.2.1 "*Vulnerability of the financial market*".

Risk occurrence scenarios (i.e. possible risk occurrence examples) both for money laundering and terrorism financing – referred to the use of financial products in the form of a bank account, credits and loans, anonymous pre-paid cards (electronic money media issued by the foreign entities – electronic money institutions offering their products in Poland on the basis of the European passport) and transfers of funds for money laundering and terrorism financing purposes. Detailed description is presented in the scenarios dedicated to the specific risk area below.

Money laundering

Table 1

Type of used services, financial products	Bank account
General risk description	Using the account for allocating and transferring the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Allocating of illicit proceeds on the bank account (by cash deposits of transfers from the other accounts) for the purposes of cash withdrawals or further transferring of cash, most frequently on the accounts in the credit institutions located in the jurisdictions not complying with the international standards and recommendations on anti-money laundering and counter-terrorism financing (AML/CFT). 2. Using the bank accounts kept for the actually operating companies. Transferring the illicit proceeds via a chain of bank accounts held by the affiliated business entities under the fictitious titles (for example payments for services or loans or their repayments), in order to separate them from the original source of origin.

	3. Using the bank accounts opened by dummy persons (straw men) or by not actually operating companies (shell companies) to make transactions with the use of illicit proceeds. 4. Opening the bank accounts for a foreign legal person (in particular registered in a tax haven) and using these accounts for the purposes of cash deposits and withdrawals as well as transfers from and to foreign bank accounts to hide the illegitimate source of funds used in these transactions. 5. Opening the bank accounts by natural persons on the basis of false ID card. Using the account to introduce the illicit proceeds to the banking system and their further transferring. 6. Making the bank accounts available to the customers by the banks offering the service of creating the individual virtual accounts (*collect* accounts), used to identify the incoming payments. The service is dedicated for the corporate customers with a large number of counterparties and receiving many payments from, for example, natural persons. This service can be used for conducting a fictitious business activity in the area of loan frauds. The individual bank accounts are assigned to the individual borrowers to collect the reservation fees i.e. the arrangement commissions for the examination of the loan application. The funds allocated on virtual accounts are then – as a batch file and automatically – transferred onto the current account of the customer and then on the following bank accounts or withdrawn in cash. 7. Using the bank account by the persons purporting to be the Ukrainian refugees, being actually the members of an international criminal organisation. The units of this organisation are located among others in Poland. The financial flows made via these accounts are associated with the crime of money laundering.
Level of vulnerability	3
Justification for the level of vulnerability	Opening of a bank account and making transactions – including of international nature – via this account is relatively easy. It is important to have access to the account via electronic communication channels (including via Internet) – using so called straw men or shell companies to open the account. According to data provided in the Report[2] "PRNews.pl: Rynek kont osobistych – I kw. 2022 r." (*PRNews.pl: Personal account market – 1Q of 2022*), the universal banking segment operates currently as many as 35.6 million of savings and settlement accounts. The greatest number of accounts is serviced by such banks as: PKO BP, Pekao and Santander. Compared to data from the end of 2021, the account market increased by 394 thousand and compared to data from a year before by nearly 1.7 million. The greatest number of personal accounts remains at PKO BP – 8.7 million. The second place in the ranking is occupied by Bank Pekao – 4.6 million, followed by Santander – 4.2 million. The same three banks recorded the highest increase in the number of accounts in the last year. According to data published by the National Bank of Poland (NBP), at the end of 2021 there were 43.3 million of payment cards. This means that in the last quarter of 2021 the number of cards increased by 470 thousand. The average value of a single transaction was PLN 123. Only in the fourth quarter of 2021 there were 2.1 billion of transactions made with payment cards for the total value of PLN 254.98 billion. Non-cash transactions accounted for more than 93% of all transactions. In the fourth quarter of 2021, the number of withdrawals from ATMs dropped by 6.8%. The average withdrawal amounted to PLN 738, while the value of transactions mde with cards in the Internet increased by PLN 1.15 billion, i.e. by 19% compared to the preceding quarter. All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area.

[2] https://prnews.pl/raport-prnews-pl-rynek-kont-osobistych-i-kw-2022-465248, access on 25.06.2022

	With regard to pending military conflict in Ukraine, proper identification and verification of the Ukrainian refugees, interested in using the products available on the financial market, poses a particular challenge related to the proper application of customer due diligence measures. Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons having no documents at all or having documents such as internal passport in Cyrillic. Correct transcription of such documents into Latin alphabet is extremely hindered. In addition, the language and cultural barrier between the obligated institutions' staff and the refugees using the bank account makes identification of untypical customer behaviours difficult, which refers both to a customer willing to open for example a bank account and the customer making a transaction. The language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. The obligated institutions are aware of their AML/CFT obligations. Although they effectively analyse the transactions, the staff of the obligated institutions performing the AML/CFT obligations in the time of the military conflict in Ukraine has been generally assigned with the tasks consisting in the application of sanctions imposed on Russia and Belarus. This leads to the situation, in which the AML/CFT tasks in the obligated institutions have been actually performed by less persons than before the conflict, which can be insufficient to properly perform these AML/CFT tasks. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU Member States, in particular as regards the entities of complicated capital structure. The public administration authorities have knowledge on the money laundering and terrorism financing (ML/FT) risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. In 2021, the total number of suspicious activity reports (SARs) from the cooperating units (CUs) recorded in the GIFI system amounted to 251[3], which demonstrates the increase compared to 2020, when the number of recorded SARs amounted to 179. In 2021, the GIFI recorded 3574 SARs from the obligated institutions. Their number remains at a high level and is by approx. 20% higher compared to the 2014-2018 average. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Using the transactions made via opened bank accounts, both the corporate and personal accounts, for the purposes of money laundering seems relatively frequent. This method is commonly available and its use is relatively inexpensive. Making transactions on the bank accounts requires neither specialist knowledge nor skills. Although customer due diligence poses certain risk to the entities allocating or transferring the illicit proceeds via a bank account, it is mitigated by the perpetrators in various ways, for example by the use of "straw men" or "shell companies" or by a forger of documents, which are difficult to verify by the bank.

[3] REPORT of the General Inspector of Financial Information on the implementation of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2021, p. 43, available at: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej. The number applies to all suspicious activity reports - ML and FT.

	The GIFI records many cases of using the bank accounts for money laundering purposes. CONCLUSION: Using a bank account for allocating and transferring the illicit proceeds poses a very high threat of money laundering.

Table 2

Type of used services, financial products	Credits and loans
General risk description	Obtaining credits and loans and their repayment with the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Incurring the consumer credits and loans, which are then relatively quickly (before the credit/loan repayment date) repaid with the illicit proceeds. 2. Taking the credits for purchasing real estates/movable assets, frequently at inflated prices, by the dummy persons (straw men). The funds from credits are transferred to the sellers of the real estates/movable assets cooperating with the perpetrators. The credits are repaid with the illicit proceeds.
Level of vulnerability	3
Justification for the level of vulnerability	Access to credits and loans granted by the banks is simple. However, due to the pending military conflict in Ukraine, customer due diligence measures related to proper identification and verification of identify of the Ukrainian refugees interested in the products available on the financial market, is hindered. In some cases, the problem lies in obtaining a broader spectrum of documents confirming the identity or reliability of such customer. Nonetheless, there are certain restrictions in entering into the credit o loan agreement associated primarily with the creditworthiness of the customer and whether the customer has adequate securities. Therefore, using the straw men or shell companies for taking credits and loans is hindered. The credits and loans can be also repaid by means of international transactions, including with the use of third persons or entities. According to data of the Credit Information Bureau[4] - in May 2022 the banks and cooperative savings and credit unions granted more (+1.5%) cash loans only compared to May. Drops were recorded in the remaining types of credits. The number of granted mortgage loans (-43.3%), credit card limits (-29.3%), and instalment loans (-4.7%) decreased. In terms of value, the banks and cooperative savings and credit units assigned lower value to all credit products. The highest decrease in value was recorded in the mortgage loans (-38.6%). Credit card limits (-16.3%), instalment loans (-3.9%) and cash loans (-0.8%) were granted for a lower value. In the first five months of 2022 the negative dynamics in both terms were recorded for credit cards (-34.0% and -16.7%) and mortgage loans (-27.9% and -19.7%) compared to the same period in the previous year, while the positive dynamics were recorded for instalment loans. (+17.4% and +2.7%) and cash loans (+5.1% and +2.4%). All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. They are aware of their AML/CFT obligations. They analyse the transactions effectively – the greatest number of SARs submitted to the GIFI comes from the banks/units of credit institutions/foreign banks' branches. In response to the COVID-19 pandemic, the obligated institutions, were forced to quickly adapt their sales systems to the requirements in the area of anti-money laundering and counter-terrorism financing to maintain their products sales. This was primarily associated with deployment of technological solutions enabling distribution of

[4] https://media.bik.pl/informacje-prasowe?offset=0, access on 25.06.2022

	products in the distance selling system. There have been also problems with verification of foreign customers in the central registers of beneficial owners of the EU Member States, which applies in particular to the entities of complicated capital structure. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2
Justification for the level of threat	Making use of the possibilities of entering into a credit or loan agreement and their repayment with the illicit proceeds are not perceived in Poland as an attractive money laundering method. As regards mortgage loans, the threat of using them for money laundering purposes is based also on the opportunity to set the prices of real estates deviating from the market prices and on the opportunity to submit tax returns in various tax offices (depending on the declared place of residence). The offenders using this method are well prepared to providing false documentation, while the limited property right such as mortgage supports hiding the actual beneficiary of the funds. In many cases, the borrower is the entities located in so called "tax havens". This *modus operandi* requires however planning, certain knowledge and skills. The GIFI has received information on applying this method of money laundering. CONCLUSION: Entering into a credit or loan agreement and their repayment with the illicit proceeds constitutes a high threat of money laundering.

Table 3

Type of used services, financial products	Anonymous pre-paid cards – electronic money media issued by the foreign entities – electronic money institutions offering their products in Poland on the basis of the European passport
General risk description	Using the anonymous pre-paid cards to impede identification of money laundering perpetrators
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The anonymous pre-paid cards are credited by the perpetrators with the illicit proceeds. The pre-paid card account is then used to make transfers onto the accounts of the other persons for the purposes of cash withdrawals or further transfers. 2. The anonymous pre-paid cards are credited by the perpetrators with the illicit proceeds. The pre-paid cards are then use to purchase various goods, which are then resold to the other persons. 3. The anonymous multi-currency pre-paid cards of a non-banking payment institution are credited by the perpetrators with the illicit proceeds. The account of the anonymous multi-currency pre-paid card is then used to make transfers onto the accounts of the other persons for the purposes of cash withdrawals or further transfers. 4. Using of pre-paid cards by the persons purporting to be the Ukrainian refugees. These persons are actually the organised crime group members. The anonymous pre-paid cards are transported between, for example, the EU territory and third countries, where at the final stage the funds deposited earlier on the anonymous pre-paid cards are withdrawn.
Level of vulnerability	2

Justification for the level of vulnerability	Access to pre-paid cards being electronic money medium is relatively easy (via Internet). The main source of money laundering risk is the anonymous pre-paid cards offered in Poland, yet issued the insurers from the other EU Member States. There is an option of withdrawing electronic money legally (saved on the pre-paid card or a server), without identifying and verifying the customer, however subject to certain limits of amounts kept on a payment instrument and limits of transactions amounts provided for in the Directive 2018/843[5]. Electronic money and pre-paid cards may be used to make international transactions. Due to supervision over the foreign electronic money institutions offering their products and services in Poland by the authorities of the home country belonging to the EU, one should assume that they have implemented and apply the applicable procedures for anti-money laundering and counter-terrorism financing (it should be remembered however that these are not the obligated institutions in the meaning of the Polish legislation, unless they operate by a branch established in Poland). According to information of the National Bank of Poland (NBP)[6] at the end of the 2nd quarter of 2022 the number of pre-paid cards in Poland amounted to 1.95 million compared to 2.25 million in the 2nd quarter of 2021 (drop by 13.33%). The share of pre-paid cards on the market as of the end of the 2nd quarter of 2022 reached 4.5%. i.e.by 0.6% less compared to the same period of the previous year. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect[7] and analyse information, however GIFI is largely dependent on information obtained from the foreign financial intelligence units. It is probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1
Justification for the level of threat	The national banks issue only the pre-paid cards being a type of debit cards. The anonymous pre-paid cards – electronic money media are issued by the electronic money institutions from the other EU Member States and offered to the customers in Poland. One should assume that the risk of money laundering may refer primarily to the cards, which are acquired by natural persons. This requires knowledge on the offer of the foreign electronic money institutions from the perpetrators. There is information originating mostly from the abroad that this *modus operandi* is used for the money laundering purposes CONCLUSION: The use of anonymous pre-paid cards to impede identification of persons making the transactions related to money laundering is currently at a low level of threat in Poland.

[5] I.e. Directive of the European Parliament and of the Council (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ EU L 156 of 19.06.2018, p. 43).

[6] https://webcache.googleusercontent.com/search?q=cache:WD2NBBEHU3gJ:https://www.nbp.pl/home.aspx%3Ff%3D/systemplatniczy/karty/informacje_kwartalne.html&cd=2&hl=pl&ct=clnk&gl=pl

[7] Pursuant to Article 53(1) of Directive 2015/849, when a financial intelligence unit receives a suspicion transaction report which concerns another EU Member State (for example Poland), it shall promptly forward it to the FIU of that Member State.

Table 4

Type of used services, financial products	Transfers of funds
General risk description	Use of transfers of funds to the other jurisdictions
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Use of transfers of funds under a fictitious title (among others to help the family). The funds are transferred in particular to the banks located in Europe and in so called tax havens. 2. A bank officer cooperating with the offenders, accepts the illegal cash proceeds from them, which are then transferred by means of non-cash transfers on the designated bank accounts, hiding their source and intended use. 3. Transferring funds to the other countries by the persons purporting to be the Ukrainian refugees and being actually the international organised crime group members. At the final stage of a financial operation, the funds are withdrawn in cash or are further transferred between the criminal group members. 4. Accepting and ordering acquisition or disposal of financial instruments onto the account of the ordering entity and/or performing the financial advisory services by the entity holding no relevant licence.
Level of vulnerability	3
Justification for the level of vulnerability	Ordering transfers of funds via the banks is relatively easy. A part of banks provides also the money transfer services on behalf of the foreign payment institutions. There is a limited number of products facilitating anonymous transactions (alternatively, it is possible in the event of occasional transactions below the level of equivalence of EUR 1 thousand or using a straw man or a shell company). Transfers of funds are frequently of international nature. All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. With regard to pending military conflict in Ukraine, proper identification and verification of the Ukrainian refugees, interested in using the products available on the financial market, poses a particular challenge related to the proper application of customer due diligence measures. Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons having no documents at all or having documents such as internal passport in Cyrillic. Correct transcription of such documents into Latin alphabet is extremely hindered. In addition, the language and cultural barrier between the obligated institutions' staff and the refugees using the bank account makes identification of untypical customer behaviours difficult, in particular of a customer willing to transfer the funds. The language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. The obligated institutions are aware of their AML/CFT obligations. Although they effectively analyse the transactions, the staff of the obligated institutions performing the AML/CFT obligations in the time of the military conflict in Ukraine has been generally assigned with the tasks consisting in the application of sanctions imposed on Russia and Belarus. This leads to the situation, in which the AML/CFT tasks in the obligated institutions have been actually performed by less persons than before the conflict, which can be insufficient to properly perform these AML/CFT tasks. However, the greatest number of SARs submitted to the GIFI comes from the banks/branches of the credit institutions/branches of the foreign banks. OIs face also problems with

	verification of the foreign customers in the central registers of beneficial owners of the EU Member States, which refers in particular to the entities of complicated capital structure. Pursuant to the study of the National Bank of Poland entities "Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2021 r." (*Comparison of the selected elements of the Polish payment system with the systems of the other European Union countries for 2021),* the total number of transfers amounted to approx. 4.03 billion[8] in 2021, while approx PLN 3.6 billion in 2020 (decrease by 0.64%). In 2021, Poland was ranked 13th among the EU states in terms of the number of transactions with payment instruments per capita.[9] Compared to data for 2020, Poland maintained its position in the EU states ranking. The number of transactions per capital in 2021 was 301, which compared to the EU average and Eurozone average (318 and 330 transactions, respectively) translates into continuously relatively low use of non-cash payment instruments in our country. One should note however that the number of transactions with non-cash payment instruments per capita increased in 2021 in Poland by as many as 19.0% compared to 222, compared to 11.3% increase in the Eurozone and 11.9% in the European Union. All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Money laundering by means of using the transfers for the purposes of money remittances to the other jurisdictions is one of the most commonly applied method. Due to well-developed global banking system, this method is widely available and relatively inexpensive. Although ordering transfers requires neither knowledge on the banking system, nor specialist skills, the execution of this *modus operandi* is relatively safe when the bank – due to the nature or place of transaction is not obliged to apply the enhanced due diligence measures. Avoiding this threat includes for example obtaining a bank officer for cooperation. If the organised crime group establishes the system of fictitious entities holding the bank accounts in the country and abroad, it can make transfers and payments between these entities, which will not be suspicious from the economic point of view and will be very difficult to challenge. Using transfers for the purposes of money remittances to the other jurisdictions in the banking system is easy and requires neither complicated planning, nor specialist knowledge or skills. CONCLUSION: Use of transfers for the purposes of money remittances to the other jurisdictions poses a very high threat of money laundering.

[8]Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2021 r., NBP, December 2022, p. 33, available at: https://www.nbp.pl/SystemPlatniczy/Obrot_bezgotowkowy/Obrot_bezgotowkowy.html

[9] Ibidem, p. 34.

Terrorism financing

Table 5

Type of used services, financial products	Bank account
General risk description	Using the account for allocating and transferring the funds for the purposes of terrorist activity
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Collecting on ban accounts of funds acquired in various ways (from legitimate and illegitimate sources) for the purposes of their further withdrawal in cash (frequently in the countries bordering the countries of operation of terrorist organisation) or transferring, most frequently onto the accounts in the credit institutions located near the conflict zones o in the jurisdictions not complying with the international AML/CFT standards and recommendations. 2. Transfer of assets from a company controlled by the terrorist organisation supporters, which then files for bankruptcy. The assets, in this case money, are transferred via a chain of bank accounts held by the affiliated entities for the purpose of their withdrawal in cash. 3. Using the bank accounts of natural persons associated with terrorists (family and other relatives) for the purposes of cash deposits followed by cross-border transfers. 4. Opening the bank accounts for the purposes of a foreign corporate person (registered in particular in a tax haven), followed by using these accounts to transfer funds to the business entities located in the area of high terrorist organisation activity (e.g. Libya, Iraq). 5. Opening bank accounts in the bank branches by natural persons on the basis of a false ID card. Opening the bank accounts via Internet, infoline or a mobile app using false data, followed by using such account to transfer funds to the persons associated with terrorist activity. 6. Self-financing of terrorists (in particular "lone wolves") from own funds collected on a bank account (frequently from legitimate sources – earnings, benefits, credits/loans, scholarships, donations from the family). 7. Transfer of funds intended for terrorist activity purposes from the bank located in Asia on the bank account in the credit institution in Europe. The account belongs to a member or supporter of a terrorist organisation, or an entity controlled by such organisation, and the transfer of funds is made by the agency of correspondent banks located in South America, which impedes identification and verification of data of transfer ordering entity. 8. Using the bank account by an entity, beneficial owner of which is a person entered into the international sanction lists or associated with a terrorist organisation or supporting it. 9. Using a bank account by the Ukrainian refugees being the members or supporters of one of the pan-Islamic and fundamentalist organisations of international range. Such organisation opts for reinstitution of caliphate covering the entire Muslim world. The units of such organisation have also occurred in Poland. Such organisation legally operates in Ukraine, but its fractions are banned by the certain European states. The financial transfers made via these accounts may be linked to the financing of terrorism.
Level of vulnerability	3

Justification for the level of vulnerability	Opening of a bank account and making transactions – including of international nature – via this account is relatively easy. It is important to have access to the account via electronic communication channels (including via Internet) – using so called straw men or shell companies to open the account. According to data provided in the Report[10] "Rynek kont osobistych – I kw. 2022 r." (*PRNews.pl: Personal account market – 1Q of 2022*) the universal banking segment operates currently as many as 35.6 million of savings and settlement accounts. The greatest number of accounts is serviced by such banks as: PKO BP, Pekao and Santander. Compared to data from the end of 2021, the account market increased by 394 thousand and compared to data from a year before by nearly 1.7 million. The greatest number of personal accounts remains at PKO BP – 8.7 million. The second place in the ranking is occupied by Bank Pekao – 4.6 million, followed by Santander – 4.2 million. The same three banks recorded the highest increase in the number of accounts in the last year. According to data published by the National Bank of Poland (NBP), at the end of 2021 there were 43.3 million of payment cards. This means that in the last quarter of 2021 the number of cards increased by 470 thousand. The average value of a single transaction was PLN 123. Only in the fourth quarter of 2021 there were 2.1 billion of transactions made with payment cards for the total value of PLN 254.98 billion. Non-cash transactions accounted for more than 93% of all transactions. In the fourth quarter of 2021, the number of withdrawals from ATMs dropped by 6.8%. The average withdrawal amounted to PLN 738, while the value of transactions made with cards in the Internet increased by PLN 1.15 billion, i.e. by 19% compared to the preceding quarter. All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. With regard to pending military conflict in Ukraine, proper identification and verification of the Ukrainian refugees, interested in using the products available on the financial market, poses a particular challenge related to the proper application of customer due diligence measures. Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons having no documents at all or having documents such as internal passport in Cyrillic. Correct transcription of such documents into Latin alphabet is extremely hindered. In addition, the language and cultural barrier between the obligated institutions' staff and the refugees using the bank account makes identification of untypical customer behaviours difficult, which refers both to a customer willing to open for example a bank account and the customer making a transaction. The language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. The obligated institutions are aware of their AML/CFT obligations. Although they effectively analyse the transactions, the staff of the obligated institutions performing the AML/CFT obligations in the time of the military conflict in Ukraine has been generally assigned with the tasks consisting in the application of sanctions imposed on Russia and Belarus. This leads to the situation, in which the AML/CFT tasks in the obligated institutions have been actually performed by less persons than before the conflict, which can be insufficient to properly perform these AML/CFT tasks. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU Member States, in particular as regards the entities of complicated capital structure. The public administration authorities have knowledge on the money laundering and terrorism financing (ML/FT) risk in this scope. The GIFI is capable to collect

[10] https://prnews.pl/raport-prnews-pl-rynek-kont-osobistych-i-kw-2022-465248, accessed on 25 June 2022

	and analyse information. It is highly probable that the case of terrorism financing in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. In 2021, the total number of suspicious activity reports (SARs) from the cooperating units (CUs) recorded in the GIFI system amounted to 251[11], which demonstrates the increase compared to 2020, when the number of recorded SARs amounted to 179. In 2021, the GIFI recorded 3574 SARs from the obligated institutions. Their number remains at a high level and is by approx. 20% higher compared to the 2014-2018 average. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Terrorism financing by means of the opened ban accounts, both corporate and personal, is one of the simplest methods to be used. The accounts may be credited both with legitimate and illegitimate funds. This method – due to well-developed banking system - is commonly available and its use is relatively inexpensive. Making transactions on the bank accounts requires neither specialist knowledge nor skills. Using the banking system and in particular the bank accounts is easy and requires no complicated planning due to the opportunities to make quick crediting and debiting transactions with them. If the terrorist organisation establishes the system of fictitious entities holding the bank accounts in the country and abroad, it can make transfers and payments between these entities, which will not be suspicious from the economic point of view and will be very difficult to challenge. Hiding the true intended use of the funds in a large number of legal transactions is relatively easy, in particular in the case of transactions of relatively low values. According to the GIFI information, this *modus operandi* can be used for terrorism financing. CONCLUSION: Using a bank account for collecting and transferring funds to terrorists poses a very high threat of terrorism financing.

Table 6

Type of used services, financial products	Credits and loans
General risk description	Incurring the loans or credits in the financial institutions without any intention to repay the liabilities
Risk occurrence scenario (i.e. possible risk occurrence example)	Incurring short- or long-term loans by natural persons, allowing for providing financial support to the terrorists, in particular for travelling to the conflict zone to join the foreign terrorist fighters.
Level of vulnerability	3
Justification for the level of vulnerability	Access to credits and loans granted by the banks is simple. However, due to the pending military conflict in Ukraine, customer due diligence measures related to proper identification and verification of identify of the Ukrainian refugees interested in the products available on the financial market, is hindered. In some cases, the problem lies in obtaining a broader spectrum of documents confirming the identity or reliability of such customer. Nonetheless, there are certain restrictions in entering into the credit o loan agreement associated primarily with the creditworthiness of the customer and whether the customer has adequate securities. Therefore, using the straw men or shell companies for taking credits

[11] REPORT of the General Inspector of Financial Information on the implementation of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism in 2021, p. 43, available at: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej. The number applies to all suspicious activity reports - ML and FT.

	and loans is hindered. The credits and loans can be also repaid by means of international transactions, including with the use of third persons or entities. According to data of the Credit Information Bureau[12] - in May 2022 the banks and cooperative savings and credit unions granted more (+1.5%) cash loans only compared to May. Drops were recorded in the remaining types of credits. The number of granted mortgage loans (-43.3%), credit card limits (-29.3%), and instalment loans (-4.7%) decreased. In terms of value, the banks and cooperative savings and credit units assigned lower value to all credit products. The highest decrease in value was recorded in the mortgage loans (-38.6%). Credit card limits (-16.3%), instalment loans (-3.9%) and cash loans (-0.8%) were granted for a lower value. In the first five months of 2022 the negative dynamics in both terms were recorded for credit cards (-34.0% and -16.7%) and mortgage loans (-27.9% and -19.7%) compared to the same period in the previous year, while the positive dynamics were recorded for instalment loans. (+17.4% and +2.7%) and cash loans (+5.1% and +2.4%). All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. They are aware of their AML/CFT obligations. They analyse the transactions effectively – the greatest number of SARs submitted to the GIFI comes from the banks/units of credit institutions/foreign banks' branches. In response to the COVID-19 pandemic, the obligated institutions, were forced to quickly adapt their sales systems to the requirements in the area of anti-money laundering and counter-terrorism financing to maintain their products sales. This was primarily associated with deployment of technological solutions enabling distribution of products in the distance selling system. There have been also problems with verification of foreign customers in the central registers of beneficial owners of the EU Member States, which applies in particular to the entities of complicated capital structure. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of terrorism financing in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	Incurring loans or credits in the financial institution without any intention to repay the liabilities may be perceived in Poland as a relatively attractive method of terrorist crime financing. This applies in particular to the consumer loans and credits rather than mortgage loans. Simplified procedures of obtaining such credits and loans, large range of banks and loan companies affects the attractiveness of this *modus operandi*. It requires no specialist knowledge, planning or unique skills from the terrorist organisation members or their supporters. Some cases may however require forging the documentation. Information on the use of this *modus operandi* for terrorism financing comes primarily from the abroad. CONCLUSION: Incurring loans or credits in the financial institutions without any intention to repay the liabilities constitutes a high threat of terrorism financing.

Table 7

Type of used services, financial products	Anonymous pre-paid cards – electronic money media issued by the foreign entities – electronic money institutions offering their products in Poland on the basis of the European passport

[12] https://media.bik.pl/informacje-prasowe?offset=0, access on 25.06.2022

General risk description	Using the pre-paid cards to impede identification of persons making the transaction associated with terrorism financing
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The funds allocated for terrorism financing are transferred between the natural persons with the use of pre-paid cards ensuring anonymity of both the card purchaser and beneficiaries of funds allocated on that card. 2. Sponsoring of terrorist activity by purchasing the anonymous pre-paid cards of international range (including the cards for international calls, online gaming) and providing the card number to persons associated with terrorists. The card (namely its description and number) is sold by the above-mentioned persons and the obtained funds are used to finance criminal activity. 3. The funds used for crediting of the anonymous pre-paid cards by different persons, are then transferred onto various accounts held or controlled by the terrorists or withdrawn in cash. 4. Using the electronic money wallets by the terrorists for the purposes of allocating funds under different titles, including for charity purposes, and then crediting the payment cards with these funds (including anonymous pre-paid cards), from which these funds are withdrawn in cash.
Level of vulnerability	2
Justification for the level of vulnerability	Access to pre-paid cards being the electronic money medium is relatively easy (via Internet). The main source of terrorism financing risk is the anonymous pre-paid cards offered in Poland, yet issued the issuers from the other EU Member States. There is an option of withdrawing electronic money legally (saved on the pre-paid card or a server), without identifying and verifying the customer, however subject to certain limits of amounts kept on a payment instrument and limits of transactions amounts provided for in the Directive 2018/843[13]. Electronic money and pre-paid cards may be used to make international transactions. Due to supervision over the foreign electronic money institutions offering their products and services in Poland by the authorities of the home country belonging to the EU, one should assume that they have implemented and apply the applicable procedures for anti-money laundering and countering the financing of terrorism (it should be remembered however that these are not the obligated institutions in the meaning of the Polish legislation, unless they operate by a branch established in Poland). The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect[14] and analyse information, however GIFI is largely dependent on information obtained from the foreign financial intelligence units. It is probable that the case of terrorism financing in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent
Level of threat	1

[13] I.e. Directive of the European Parliament and of the Council (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ EU L 156 of 19.06.2018, p. 43).
[14] Pursuant to Article 53(1) of Directive 2015/849, when a financial intelligence unit receives a suspicion transaction report which concerns another EU Member State (for example Poland), it shall promptly forward it to the FIU of that Member State.

Justification for the level of threat	The national banks issue only the pre-paid cards being a type of debit cards. The anonymous pre-paid cards – electronic money media are issued by the electronic money institutions from the other EU Member States and offered to the customers in Poland. One should assume that the risk of terrorism financing may refer primarily to the cards, which are acquired by natural persons. This requires knowledge on the offer of the foreign electronic money institutions from the perpetrators. There is information originating mostly from the abroad that this *modus operandi* is used for the terrorism financing purposes. CONCLUSION: The use of anonymous pre-paid cards to impede identification of persons making the transactions related to terrorism financing is currently at a low level of threat in Poland.

Table 8

Type of used services, financial products	Transfers of funds
General risk description	Use of transfers of funds to the other jurisdictions
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Use of transfers of funds under a fictitious title (among others to help the family). The funds are transferred to the banks located in the counties bordering with the place of activity of terrorist organisations. 2. A bank officer cooperating with the terrorists accepts the illegal cash proceeds from them or their supporters, which are then transferred by means of non-cash transfers on the designated bank accounts, hiding their source and intended use. 3. Transferring funds by the Ukrainian refugees, being the members or supporters of one of the Pan-Islamic and fundamentalist organisations of international range (opting in their programme for reinstitution of caliphate covering the entire Muslim world and operating legally in Ukraine) to the other countries, where these organisations are banned. The transfers of funds involving the members or supporters of this organisation may be directly or indirectly linked to terrorism financing.
Level of vulnerability	3
Justification for the level of vulnerability	Ordering transfers of funds via the banks is relatively easy. A part of banks provides also the money transfer services on behalf of the foreign payment institutions. There is a limited number of products facilitating anonymous transactions (alternatively, it is possible in the event of occasional transactions below the level of equivalence of EUR 1 thousand or using a straw man or a shell company). Transfers of funds are frequently of international nature. All the above-mentioned products/services providers are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. With regard to pending military conflict in Ukraine, proper identification and verification of the Ukrainian refugees, interested in using the products available on the financial market, poses a particular challenge related to the proper application of customer due diligence measures. Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons having no documents at all or having documents such as internal passport in Cyrillic. Correct transcription of such documents into Latin alphabet is extremely hindered. In addition, the language and cultural barrier between the obligated institutions' staff and the refugees using the bank account makes identification of untypical customer behaviours difficult, in particular of a customer willing to transfer the

	funds. The language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. The obligated institutions are aware of their AML/CFT obligations. Although they effectively analyse the transactions, the staff of the obligated institutions performing the AML/CFT obligations in the time of the military conflict in Ukraine has been generally assigned with the tasks consisting in the application of sanctions imposed on Russia and Belarus. This leads to the situation, in which the AML/CFT tasks in the obligated institutions have been actually performed by less persons than before the conflict, which can be insufficient to properly perform these AML/CFT tasks. However, the greatest number of SARs submitted to the GIFI comes from the banks/branches of the credit institutions/branches of the foreign banks. OIs face also problems with verification of the foreign customers in the central registers of beneficial owners of the EU Member States, which refers in particular to the entities of complicated capital structure. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Money laundering by means of using the transfers for the purposes of money remittances to the other jurisdictions is one of the most commonly applied method. Due to well-developed global banking system, this method is widely available and relatively inexpensive. Although ordering transfers requires neither knowledge on the banking system, nor specialist skills, the execution of this *modus operandi* is relatively safe when the bank – due to the nature or place of transaction is not obliged to apply the enhanced due diligence measures. Avoiding this threat includes for example obtaining a bank officer for cooperation. If the organised crime group establishes the system of fictitious entities holding the bank accounts in the country and abroad, it can make transfers and payments between these entities, which will not be suspicious from the economic point of view and will be very difficult to challenge. Using transfers for the purposes of money remittances to the other jurisdictions in the banking system is easy and requires neither complicated planning, nor specialist knowledge or skills. CONCLUSION: Use of transfers for the purposes of money remittances to the other jurisdictions for terrorist activity poses a very high threat of money laundering.

The COVID-19 pandemic has led to major changes in the operation model of the banks, cooperative banks or cooperative savings and credit unions. The number of active users of banking services available via electronic access channels and the number of cashless (contactless) transactions and electronic payments have significantly increased. At the same time, Poland faced a paradox in 2022 – the value of currency in circulation continues to grow despite the fact that as a legal tender it has been regularly displaced by the other forms of payments[15]. In April 2022, currency in circulation accounted for 18.7% of broad supply of money (M3) and 12.4% of annual GDP. In 2009, cash payments were preferred by

[15]Analysis of PeKaO S.A. - https://www.wnp.pl/finanse/paradoksalna-sytuacja-gotowka-zalewa-polski-rynek,587245.html, access on 10.12.2022

64% of the Poles, while in 2021 this percentage dropped down to 21%. In 2013, as many as 70% of transactions of the value between PLN 11-50 were made in cash, while currently its share decreased to 1/3.

Vulnerability of the sector

All products and services providers in the banking sector are the obligated institutions (OIs). This applies to the commercial banks, cooperative banks or cooperative savings and credit unions. These entities are obliged to apply customer due diligence measures. The controls performed in this area reveal however certain errors and deficiencies. Customer due diligence measures set out in the Act cover primarily the activities related to identification of the customer and verification of its identity; identification of beneficial owner and taking reasonable measures to verify its identity and determine the ownership and control structure in the case of a customer being a legal person or an organisational unit without legal personality. In addition, the banking sector entities assess the business relationships of the customer and (as appropriate) obtain information on their purpose and intended nature. The banking sector entities are aware of their AML/CFT obligations. They analyse the transactions effectively – the greatest number of suspicious transaction reports submitted to the General Inspector of Financial Information (GIFI) comes from the banks/units of credit institutions/foreign banks' branches. According to the GIFI data on the analytical proceedings initiated by the GIFI in 2019-2021, vast majority of these proceedings was related to the suspicion of money laundering or terrorism financing with regard to the use of bank accounts for suspicious transactions. In 2019, these accounted for approx. 81.5% of proceedings related to the suspicion of money laundering or terrorism financing with regard to the use of bank accounts for suspicious transactions. In 2020, these accounted for approx. 74.8%, while in 2021 of approx. 85.0%. A relatively high level of reporting on the suspicion of money laundering by the banking sector employees results from the fact that the sector has strong awareness of exposure to the crime of money laundering and terrorism financing and that the sector employees are trained in analysing the warning signals triggered by suspicious transactions. According to information held by the GIFI, the banking sector institutions hold the advanced tools and IT systems supporting the implementation of the objectives of anti-money laundering and counter-terrorism financing. To this end, these institutions use for example the systems supporting the transaction process analysis or the systems dedicated to customer verification with a view to the sanctions lists. In addition, the GIFI has carried out trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of customers as well as reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) were provided. The trainings raising the AML/CFT awareness in the obligated institutions are also carried out. These trainings are organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme.

One should note however that with regard to pending military conflict in Ukraine, proper identification and verification of the Ukrainian refugees, interested in using the products available on the financial market, poses a particular challenge related to the proper application of customer due diligence measures. Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons having no documents at all or having documents such as internal passport in Cyrillic. Correct transcription of such documents into Latin alphabet is extremely hindered. In addition, the language and cultural barrier between the obligated institutions' staff and the refugees using the bank account makes identification of untypical customer behaviours difficult, which refers both to a customer willing to, for example, open for example a bank account and the customer making a transaction. The

language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents.

The public administration authorities have knowledge on the money laundering and terrorism financing (ML/FT) risk in this scope. The GIFI is capable to collect and analyse information. It is probable that the case of money laundering or terrorism financing in the scope of the scenarios analysed for the banking sector area will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. In 2021, GIFI recorded 3574 SARs from the obligated institutions in general. Their number remains at a high level and is by approx. 20% higher compared to the 2014-2018 average. Nevertheless, the staff of the obligated institutions, including the banking sectors institutions, performing the AML/CFT obligations in the time of the military conflict in Ukraine have been generally assigned with the tasks consisting in the application of sanctions imposed on Russia and Belarus. This leads to the situation, in which the AML/CFT tasks in the obligated institutions have been actually performed by less persons than before the conflict, which can be insufficient to properly perform these AML/CFT tasks.

The PFSA identified also the cases, in which the controlled OIs failed to ensure the relevant staff number in the AML units of these institutions – there was insufficient number of staff with a view to the performed and dynamically changing duties. The consequence of the above is in particular a highly extended process of examining the alerts generated by the IT systems on the basis of the implemented scenarios, which infringes the obligations provided for in Article 43(3) and 4591)(4)(a) of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism, which oblige the OIs to perform on-going analysis of the transactions.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent..

In 2022, the GIFI performed the commercial banks' risk scoring for 13 quarters (as the reporting periods) in 2018-2021 with regard to irregularities taking place in the banks. Data on 34 banks were analysed. The scoring covered the analysis based on the following criteria: untimely submission of quarterly reports by the banks to the GIFI under Article 76 of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism; low share of PEPs in the total number of customers; low share of beneficial owners having the PEP status in the total number of PEP customers; high share of low-risk customers in the total number of customers; low share of reported cases / reports in the total number of customers; share of selected cases / reports in the total number of cases / reports; amount of negative information received via social signals channels; volume of negative information from the Analytical Departments of the GIFI received by the Control Department of the GIFI; amount of negative information received by the GIFI from the cooperating units. With a view to the above-mentioned criteria, seven banks (out of 34) were considered the institutions of high risk of irregularities. Six banks were assessed as the institutions with low risk of irregularities, while the remaining twenty one banks were classified with a view to the above-mentioned criteria as the institutions of medium risk of irregularities.

Scoring for the cooperative savings and credit unions for the period between 1Q of 2019 and 2Q of 2021 i.e. 6 reporting periods was carried out at the same time. Data on 20 CSCUs were analysed. Scoring covered the analysis based on the following criteria: share of low-risk customers in the total number of customers; share of PEPs in the total number of customers; share of beneficial owners having the PEP status in the total number of PEP customers. With a view to the above-mentioned criteria, two CSCUs

were considered the institutions of high risk of irregularities. Fifteen from among the assessed CSCUs were assessed as the institutions of medium risk of irregularities, while the remaining three CSCUs were classified with a view to the above-mentioned criteria as the institutions of low risk of irregularities.

Scoring for the same period i.e. 6 reporting periods was also performed for the cooperative banks. Data on 553 cooperative banks were analysed. Scoring covered the analysis based on the following criteria: low share of the reported cases/reports in the total number of customers; high share of low-risk customers in the total number of customers; low share of PEPs in the total number of customers; low share of PEPs in the total number of PEP customers; share of selected cases / reports in the total number of cases / reports. With a view to the above-mentioned criteria, twenty four cooperative banks were considered the institutions of high risk of irregularities. Two hundred and thirteen from among the assessed cooperative banks were assessed as the banks of medium risk o irregularities, while the remaining three hundred and sixteen cooperative banks were classified with a view to the above-mentioned criteria as the institutions of low risk of irregularities.

The commercial banks, social banks and cooperative savings and credit unions form a part of the financial market under the supervision competences of the Polish Financial Supervision Authority (PFSA). The competences of this authority are laid down in the *Act of 21 July 2006 on the financial market supervision* and in the acts governing the operation of the individual financial market sectors, i.e.: banking, insurance, pension, capital, cooperative savings and credit unions and payment services sectors. The aim of the PFSA supervision[16] over the financial market is to ensure proper operation of this market, its stability, security and transparency, trust to the financial market and to ensure the protection of interests of the participants of this market, including by reliable information on the market operation. The PFSA supervises the financial market by performing the following functions: authorising, regulatory, control and disciplinary. The PFSA issues the authorisations for the activities the banks, cooperative savings and credit unions, national payment institutions, insurance and reinsurance companies, open pension funds, investment funds or investment companies. The legislator provided the PFSA with numerous competences in the area of applying the supervisory measures[17]. For example, if any infringement of the applicable legislation is revealed, the PFSA may impose financial penalties provided for in the legislation and withdraw the authorisation for the financial institution concerned. If any market practice raises the controversies, the PFSA may issue the recommendations dedicated to the entity concerned or recommendations or guidelines affecting the entire financial market sector. The PFSA analyses the reports submitted by the financial institutions on the on-going basis and assesses whether they meet the capital requirements provided for by law. The PFSA competences include also performing the controls in the supervised entities. In 2022, the PFSA controlled 5 commercial banks and 5 cooperative banks with a view to anti-money laundering and counter-terrorism financing. In effect of control activities performed in 2022 by the Office of the PFSA in these supervised entities, 237 irregularities were identified. The most frequent irregularities and infringements included: failure to update data of the customers and their beneficial owners affecting the risk level assigned to them previously; failure to update the customer risk assessment on a periodic basis; improper determination or failure to determine the beneficial owner; failure to fulfil the obligations associated with the on-going analysis of transactions and obligations related to the analysis of transactions performed as an on-going monitoring of business relations of the customer and documenting the results of analyses of transactions; adopting the excessively distant dates for analysing the transactions and closing the alerts; insufficient scope, quality or/and frequency of management information; failure to

[16] https://www.knf.gov.pl/dla_konsumenta/Ochrona_klienta_na_rynku_uslug_finansowych/KNF, access on 14.03.2023
[17] Ibidem

reflect in the activities of staff involved in AML/CFT of all duties performed by them in this scope; infringing the principle of separation of the operational and supervisory functions in the area of AML/CFT; determining the ML/FT risk level of the obligated institution at a excessively low level with a view to the specific nature of the entity and findings made during the control activities; non-compliance of the internal regulations with the applicable law or failure to include all aspects required by the Act in their content; despite the identified irregularities in the internal control system, the scope of the internal control system fails to cover the key elements of the AML/CFT process and the actions taken to eliminate the irregularities is not sufficiently effective; failure to implement or partial implementation of the recommendations of the PFSA. In 2022, with regard to the cooperative savings and credit unions, the National Union[18] controlled four Unions in the area of anti-money laundering and counter-terrorism financing.

Threats in the sector

In terms of assessing the threat of money laundering and terrorism financing, the banking sector is the most frequently used sector with a view to predicate offences in the area of money laundering and terrorism financing: tax offences, drug trafficking, property and trading offences, corruption, human trafficking or frauds.

Both money laundering and terrorism financing using the products offered by the banking sector (for example opened bank accounts, both corporate and personal, credits and loans, anonymous pre-paid cards and transfers of funds) are one of the simplest methods. Due to well-developed banking system in Poland, this method is commonly available and its use is relatively inexpensive. Making transactions on the bank accounts requires neither specialist knowledge nor skills.

Using the banking system and especially bank accounts due to the opportunities to make quick crediting and debiting transactions with these accounts is easy and requires no complicated planning.

With regard to this sector, one should put particular attention to the risks related to the increase in crimes linked to phishing, increased risk of using so called "straw men", changes in customer behaviours related to higher number of on-line transactions and resignation from the visits in the customer service points. One should also put attention to the increased use of bank transfers for the purposes of criminal activity and changes in the volume and value of transactions. In addition, the increased number of opening the accounts and granting credits and loans for stolen identities (i.e. for the persons who have never opened these accounts and never taken such credits and loans) was identified.

The products and services particularly exposed to being used for frauds on the market or transferring/keeping the proceeds of crime include the *collect* accounts – offered by the banking sector for the financial intermediation entities. These accounts are of high risk, since they impeded identification of the ordering parties of the transaction and its actual beneficiaries. The sector covers also the sub-sectors of moderate level of risk of money laundering and terrorism financing. These include using the pre-paid cards to hinder identification of the persons making the transactions linked to terrorism financing or money laundering perpetrators.

Apart from the *collect*-type accounts offered by the banking sector to the financial intermediation entities, the areas and sectors particularly exposed to the risk of money laundering and terrorism financing in the banking sector include – in the scope of offering the products and services particularly exposed to being used for frauds on the market or transferring/keeping the proceeds of crime – in particular electronic money value transfer/money transfer service; safe deposit boxes services; products

[18] Data of the National Association of Cooperative Savings and Credit Union

and services which promote anonymity by their nature (for example bearer instruments) and instruments of unique complexity and structure without any obvious economic purpose. The areas particularly exposed to the risk of money laundering and terrorism financing in the banking sector include additionally the activity of entities providing the services in the area of the formation of legal persons, which are serviced by the financial institutions of the sector. In addition, the areas of risk include also distance establishment of business relationships without a physical presence of a customer in the obligated institution and so called outsourcing of customer due diligence by the obligated institution. Improper customer due diligence may be also linked to high fluctuation of operational staff performing duties in the area of anti-money laundering and counter-terrorism financing in the obligated institution. Exposure to the risk of money laundering and terrorism financing in the banking sector is also associated with establishing business relationships with the persons, who actually hold no assets and are used as so called straw men by the other persons/entities to hide the identity of the persons actually holding these assets. A similar risk is associated with establishing business relationships with the entities involved in so called crowdfunding. Crowdfunding promotes hiding the source of origin of funds and generates the risk of money laundering and terrorism financing for the obligated institutions, in particular in the cases of unduly performed KYC process and therefore insufficient knowledge of the financial institution on the serviced entity. Another areas and sectors particularly exposed to the risk of money laundering and terrorism financing in the banking sector include the failure to identify by the obligated institution, whether the beneficial owner of the customer is a politically exposed person, alternatively, the failure to identify by the obligated institution of the beneficial owners of the client being the citizens or resided at the territory of the state considered as a country of high risk of money laundering and terrorism financing as well as the failure to verify the beneficial owners of the customer on the sanctions lists.

In context of threats related to the potential terrorism financing, the conflict in Ukraine generates the threat to Poland related to penetration by one of the pan-Islamic and fundamentalist organisations of international range through the eastern border and potential operation in the country. This organisation opts for reinstitution of caliphate covering the entire Muslim world. The units of such organisation have also occurred in Poland, while the propaganda is addressed to the converts, migrants from the Middle East North Africa (MENA) area and the Chechens. It is highly probable, that there can be supporters of this organisation among the Ukrainian or Russian refugees, the more that before the annexation of the Crimea by Russia, this organisation has been operating there legally. This organisation has been also operating legally in several western countries, while in the United Kingdom and Germany it was banned. The financial flows involving the members of supporters of this organisation may be associated with terrorism financing. One should also note that the terrorism is financed both from legitimate and illegitimate sources. The funds are usually deposited on the bank account, saved that they come from documented, legal sources and raise no suspicions when opening a bank account, in particular when the funds crediting the accounts are paid by the persons not involved directly in terrorist activities. Such persons are among others the family and friends of persons suspected of terrorist activity. The funds are frequently withdrawn from the bank accounts via ATMs, without involving the banking sector staff. Such funds can be withdrawn by the other persons than bank account holders.

Averaged level of threat of the banking sector – ML – 2.75 and FT – 3.0

Averaged level of vulnerability of the banking sector – ML – 2.75 and FT – 2.75

Estimated level of probability for the sector – ML – 2.75 and FT – 2.85

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators

to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the banking sector s– 2.31	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the banking sector – 2.65	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the banking sector for the purposes of terrorism financing in Poland is medium.

CONCLUSION 2: The level of risk of using the banking sector for the purposes of money laundering in Poland is high.

Mitigation of the identified risks:

In order to mitigate the probability of using the banking sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The banking sector entities should continue their activities related to appropriate assessment of the business relationships of the customer and obtaining information on their purpose and intended nature as well as to maintain on-going monitoring of business relationships.

Due to the importance of the banking sector in the anti-money laundering and counter-terrorism financing system, the entities from this sector should put particular attention to the identification of factors indicating a higher risk of money laundering and terrorism financing, in particular these listed in Article 43(2) of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism. In the case of the products and services offered to the customers, including these facilitating anonymity, such as the *collect*-type services, the banks should on one hand verify the business purpose of using this

service by the customer, while on the other hand– under the on-going monitoring of transactions – they should verify the trends indicating the use of a *collect* service contrary to its intended use or its misuse.

The banking sector should undertake the actions guaranteeing maintenance of strong awareness of exposure to the crime of money laundering and terrorism financing, as well as maintaining the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

Continued development by the banking sector institutions of the advanced IT systems and tools supporting the delivery of the objectives of anti-money laundering and counter-terrorism financing is recommended.

The trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be continued. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended. Due to the identified risk linked to the use of false documents, the obligated institutions' staff involved in the identification and verification of customer identity should be trained on the on-going basis in identifying the false documents, including the documents other than Polish.

The obligated institutions should put attention to the business relationships of their customers with foreign entities, in particular when the operation and transactions of such foreign entities demonstrate no connection with the territory of Poland. The obligated institutions keeping the bank or payment accounts should put particular attention to the transfers of funds to the jurisdictions of higher risk of money laundering and terrorism financing. The focus should be in particular on cyclical transfers of funds with an enigmatic title of a payment order or repeating transfers of funds to a specific jurisdiction, without any business justification for such transfers. The obligated institutions should place particular emphasis to determination of data on the source of origin of transferred assets as well as documents justifying the specific transaction.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance.

2. Area – payment services (offered by entities other than banks)

Sector description - is contained in sub-chapter 2.1.2. of NRA "Financial market sectors" and in sub-chapter 7.2.1 "*Vulnerability of the financial market*" as well as in chapter 6.3. "The most common methods used to finance terrorism".

Risk occurrence scenarios (i.e. possible risk occurrence examples) both for money laundering and terrorism financing – referred to the use of financial products and services in the form of money transfers online payment services and Hawala transfer system for money laundering and terrorism financing purposes. Detailed description is presented in the scenarios dedicated to the specific risk area below.

Money laundering

Table 9

Type of used services, financial products	Transfers of funds
General risk description	Use of money transfer service providers for the purposes of transfer of illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using money transfer services to transfer illicit proceeds outside the country in order to use them in the other jurisdiction. 2. Using money transfers to receive foreign illicit proceeds in order to withdraw them in cash. 3. Using a wireless POS (*point of sale*) terminal for the purposes of accounting the illicit proceeds on the bank account with the use of payment cards issued by the foreign banking institutions. This activity may indicate a theft of cards of so called skimming. With regard to the use of foreign cards, determination of the source of origin of the funds is hindered. This method is applied to authenticate that the received funds derive from a legal business activity i.e. from the sales of goods/services. In this scenario, the card transactions can be used by means of contactless transactions with a mobile phone and mobile payments – Google Pay and Apple Pay.
Level of vulnerability	2
Justification for the level of vulnerability	The money transfer services are relatively easily accessible. There is a limited possibility of hiding the identification data of the ordering persons and beneficiaries of money transfers, when making the occasional transactions below the level of equivalence of EUR 1 thousand or using a straw man or a shell company. Transfers of funds are frequently of international nature. Practically all these service providers are the OIs, excluding the payment institutions from the other EU Member States providing the payment services at the territory of Poland via agents. In March 2021, Visa announced[19] launching of the real-time push payments platform with the use of Visa Direct Payouts, which enables the Visa customers and partners (P2P, B2B and B2C models) around the world transferring payments via a single connection with VisaNet onto the qualifying cards for the purposes of domestic withdrawals and qualifying cads or accounts for cross-border payments. The flexible interfaces - API Visa Direct Payouts – decrease the complexity frequently associated with money management and transferring through multiple networks and agents throughout the world. Visa Direct platform is adapted for payments in the cooperating entities' systems (to this date among others TransferWise, Western Union and Remitly), which resulted in a significant growth in the number of real-transfers

[19] Report of the National Bank of Poland (NBP): Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2021 r., p. 110.

	made via this platform. Similarly, the British FinTechTransferGo deployed the Visa Direct platform-based solution and offered their customers making cross-border money transfers in near real time onto their payment cards without the need to use online banking or entering IBAN. These entities have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed. They submit relatively small numbers of SARs. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU Member States, which refers in particular to the entities of complicated capital structure. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Using the money transfer service providers and wireless POS (*point of sale)* terminals for the purposes of transferring illicit proceeds outside the country or receiving the illicit proceeds is one of the commonly used methods of money laundering. This method is widely available and relatively inexpensive and is perceived by the perpetrators as attractive. This type of money transfers requires no bank account held by the payer. The beneficial owners are frequently hidden by straw men. Using the money transfer service providers and wireless POS (*point of sale)* terminals for the purposes of transferring illicit proceeds outside the country requires no specialist knowledge. The GIFI has received information on using this method for money laundering purposes. CONCLUSION: Using the money transfer service providers for the purposes of transfers of illicit proceeds – in a form of money transfer – outside the country or receiving the illicit proceeds poses a very high threat of money laundering.

Table 10

Type of used services, financial products	Online payment services
General risk description	Using the online payment services by the perpetrators for the purposes of transferring the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using the online payment services by the perpetrators for the purposes of transferring the illicit proceeds from the bank account, on which they were collected, and their "flipping" between different accounts opened at the payment service providers to ultimately deposit them on the bank account held by a natural person or a business entity controlled by the perpetrators. 2. The payment institution agent (or alternatively the payment institution employee) cooperating with the perpetrators accepts the illicit proceeds from them and then deposits them on the selected bank accounts using the cashless transfers, hiding their source and intended nature.
Level of vulnerability	3

Justification for the level of vulnerability	Online transfer services are relatively easily available – all you need is access to the Internet. There are possibilities to hide the identification data of a person using this type of payment services (with regard to COVID-19, many institutions enabled the transactions made to a specific amount without verification of identification data, while verification of identification data itself is simplified – based on the scan or a passport or driving licence provided by the customer, photo from an online camera and geo-location data of the customer). Transfers of funds are frequently of international nature. Innovative payment instruments and services, such as Google Pay, Apple Pay, Revolut and other continue to gain on importance on the Polish market. Only a part of these service providers is the OIs. The payment institutions providing payment services via the online platforms, registered in the other countries (apart from the branches of the EU payment institutions, branches of the EU and foreign electronic money institutions) are not the OIs. The OIs in the payment services area have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed. They submit relatively low number of SARs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2
Justification for the level of threat	Using the online payment services which enable *online* payments and money transfer via Internet, being an electronic alternative for the conventional methods, such as cheques and direct debits, is the method of money laundering, which with the General Inspector of Financial Information has been confronted, however it seems that this method is not perceived by the potential "launderers" as attractive. Excessive volume in trade may be quickly noticed. There are also the limits of the total value of transactions made in a certain period of time. There may be also difficulties in contacts with the operator in the case of any irregularities. This causes certain troubles with using this method, the more that it requires adequate planning and specialist knowledge. The GIFI has information on using this method for money laundering purposes. CONCLUSION: Using the online payment services poses a medium threat of money laundering.

Table 11

Type of used services, financial products	Hawala transfer systems
General risk description	Using the Hawala networks or other informal transfer systems for transferring the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using the illegal payment service providers for transferring the proceeds of crime. Among others, a person offering such services uses the bank accounts, which are deposited by this person with funds originating from its customers. Then these funds are transferred onto the accounts of the services providing legal payment services.

	2. Transferring the proceeds from profits of criminal organisations established by the offenders from the same region of the world outside the country. 3. The funds transferred in the money laundering process are blended with the other money transfers within the Hawala network in order to cover up traces after the transactions.
Level of vulnerability	4
Justification for the level of vulnerability	The Hawala system services facilitate making quick and anonymous transactions of international nature to a large extent. Due to the fact, that such services are provided by the entities beyond the state control – there are no data on the volume and value of transactions made under this system. These service providers are not the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information. It is probable that the case of money laundering in the scope of the analysed scenarios will not be detected. Knowledge of the law enforcement authorities on the Hawala operations stems primarily from the operational knowledge and other foreign services. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1
Justification for the level of threat	The Hawala system is a type of an informal banking system. It is used among others in the international trading, frequently to transfer funds to great distances. Its important component is the opportunity to ensure full anonymity and using several intermediaries when ordering a transfer. A person depositing cash is not asked to present any identity document and is usually unknown or poorly known to a given intermediary. Similarly, a withdrawing person may collect the delivered funds only by providing the agreed password. In this manner, an entity offering services in the Hawala system usually does not know from whom, for what and to whom it transfers the funds. The key issue is the trust between the intermediaries, who are in most cases the members of a single family, friends, or recommended persons, and operate in a few or several countries. The fact that the persons depositing and withdrawing cash do not need to hold a bank account in a given country is also of importance (in many cases, due to restrictive local banking provisions, they cannot open the account in this country). The volume of payments/trading made via such informal systems remains unknown. Applying this *modus operandi* requires knowledge on the persons offering such services. There are no numerous ethnical minorities in Poland, in which the Hawala systems are common. CONCLUSION: Using of the informal Hawala banking system for transferring the illicit proceeds poses a low threat to money laundering.

Terrorism financing

Table 12

Type of used services, financial products	Transfers of funds
General risk description	Use of money transfer service providers for the purposes of transfer of assets intended for terrorism financing
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using by the persons associated with the terrorists of the opportunities to use simplified customer due diligence at low amounts of transactions by the money transfer service providers. This enables transfers of funds in a manner impeding the identification of the ordering party and beneficiary. Cash will be deposited in Poland and withdrawn in the countries of high activity of terrorist organisations. 2. Using money transfers for the purposes of providing financial support of the foreign terrorist fighters staying or travelling to the conflict zone. 3. Using by the persons financing the terrorism of the services of the providers operating in Poland however providing no suspicious transaction reports to the Polish financial intelligence unit.
Level of vulnerability	3
Justification for the level of vulnerability	The money transfer services are relatively easily accessible. There is a limited possibility of hiding the identification data of the ordering persons and beneficiaries of money transfers, when making the occasional transactions below the level of equivalence of EUR 1 thousand or using a straw man or a shell company. Transfers of funds are frequently of international nature. Practically all these service providers are the OIs, excluding the payment institutions from the other EU Member States providing the payment services at the territory of Poland via agents. In March 2021, Visa announced[20] launching of the real-time push payments platform with the use of Visa Direct Payouts, which enables the Visa customers and partners (P2P, B2B and B2C models) around the world transferring payments via a single connection with VisaNet onto the qualifying cards for the purposes of domestic withdrawals and qualifying cads or accounts for cross-border payments. The flexible interfaces - API Visa Direct Payouts – decrease the complexity frequently associated with money management and transferring through multiple networks and agents throughout the world. Visa Direct platform is adapted for payments in the cooperating entities' systems (to this date among others TransferWise, Western Union and Remitly), which resulted in a significant growth in the number of real-transfers made via this platform. Similarly, the British FinTechTransferGo deployed the Visa Direct platform-based solution and offered their customers making cross-border money transfers in near real time onto their payment cards without the need to use online banking or entering IBAN. These entities have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed. They submit relatively small numbers of SARs. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU Member States, which refers in particular to the entities of complicated capital structure. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

[20] Report of the National Bank of Poland (NBP): Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2021 r., p. 110.

	The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	For the low-value transactions, the money transfer service providers may apply simplified customer due diligence. This enables transfer of funds from fully legitimate sources. At present, the terrorist activity is low-input (for example, in 2021, the terrorist attacks in Europe were performed only with the used of blade weapons [knifes], vehicles [for ramming purposes], and low-input improvised explosive devices). Self-financing of terrorist activity occurs in particular with respect to single fighters or small terrorist groups. Nonetheless, receiving a single or several low-value money transfers is frequently one of the common and known methods of terrorism financing. This method is widely available and relatively inexpensive and is perceived by the perpetrators as attractive. This type of money transfers requires no bank account held by the payer. The beneficial owners are frequently hidden by straw men, cooperating entities or a family. Using the money transfer service providers to transfer the legal or illegal funds requires minimum specialist knowledge on the funds transfer system, is relatively inexpensive in terms of fees and relatively secure. CONCLUSION: This information and the presence of persons from the states and regions of increased risk in Poland as well as the potential possibility of penetration through the eastern border and possible operation in the country of the members of pan-Islamic and fundamentalist organisation of international range, calling for reinstitution of caliphate covering the entire Muslim world in their programme, banned in certain EU Member States, make the use of the scheme involving the money transfer service providers for transfers of funds – in the form of money transfer for the purposes of terrorism financing - a very high threat of terrorism financing.

Table 13

Type of used services, financial products	Online payment services
General risk description	Using the online payment services by the entities involved in the terrorism financing process, in particular by the potential foreign terrorist fighters
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using the online payment services by the foreign terrorist fighters to make e-purchases of equipment necessary to stay in the conflict zone. 2. Using these services by the persons depositing funds for the purposes of charity organisations involved in the terrorism financing process. 3. Transferring funds between the individuals involved in terrorism financing. 4. Using cashless money transfers (below the threshold requiring identification of the customer) to transfer the funds under a fictitious title (among others to support the family). The funds are transferred to the payment institution agencies located in the countries bordering the site of terrorist organisations activity. 5. The payment institution agent (or alternatively the payment institution employee) cooperating with the terrorists accepts the funds from them or their supporters and then deposits them on the selected bank accounts using the cashless transfers, hiding their source and intended nature
Level of vulnerability	3

Justification for the level of vulnerability	Online transfer services are relatively easily available – all you need is access to the Internet. There are possibilities to hide the identification data o f a person using this type of payment services (with regard to COVID-19, many institutions enabled the transactions made to a specific amount without verification of identification data, while verification of identification data itself is simplified – based on the scan or a passport or driving licence provided by the customer, photo from an online camera and geo-location data of the customer). Transfers of funds are frequently of international nature. Innovative payment instruments and services, such as Google Pay, Apple Pay, Revolut and other continue to gain on importance on the Polish market. Only a part of these service providers is the OIs. The payment institutions providing payment services via the online platforms, registered in the other countries (apart from the branches of the EU payment institutions, branches of the EU and foreign electronic money institutions) are not the OIs. The OIs in the payment services area have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed. They submit relatively low number of SARs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Using the online payment services, which enable *online* payments and money transfer via Internet, being an electronic alternative for the conventional methods, such as cheques and direct debits, is a relatively attractive method of terrorism financing. The terrorist undertakings belong to relatively inexpensive investments compared to losses and panic caused. At present, there are persons from the states and regions of increased risk as well as the potential Ukrainian refugees, being the members or supporters of pan-Islamic and fundamentalist organisation of international range, calling for reinstitution of caliphate covering the entire Muslim world in their programme (banned in certain EU Member States) and operating legally in Ukraine. For these persons, the offered payment services enabling the entrepreneurs and consumers holding an e-mail address sending and receiving payments via Internet are attractive. Due to relatively low value of money transfers, such transfers may be not recorded as suspicious. In addition, they are easy to use, however require planning and knowledge. CONCLUSION: Using the online payment services poses a very high threat of terrorism financing.

Table 14

Type of used services, financial products	Hawala transfer systems
General risk description	Using the Hawala networks or other informal transfer systems for transferring assets for the purposes of terrorism financing

Risk occurrence scenario (i.e. possible risk occurrence example)	1. Depositing cash in the country X of high threat of terrorism, combined with withdrawal at the territory of Poland for the purposes of financing the terrorist activity. Using the informal network of transfers of the proceeds of crime to prevent detection of funds flow. 2. The funds transferred for terrorism financing are blended with the other money transfers within the Hawala network in order to cover up traces after the transactions. 3. Using the illegal payment service providers for transferring cash to the terrorists. Among others, a person offering such services uses the bank accounts, which are deposited by this person with funds originating from its customers. Then these funds are transferred onto the accounts of the services providing legal payment services. 4. Trusted entities in the country of a relatively low threat of terrorism receive money transfers of a relatively low one off value. The funds are sent by the families of the fighters of, for example, the Islamic State. The received amounts are transferred within the Hawala network to the countries bordering the conflict zone for terrorist purposes or back to the Foreign Terrorist Fighters. The Hawala systems use among others gold for account clearing purposes. Gold is easy to liquidate, in particular in certain Asian and African countries having well-developed gold trading markets.
Level of vulnerability	4
Justification for the level of vulnerability	The Hawala system services facilitate making quick and anonymous transactions of international nature to a large extent. Due to the fact, that such services are provided by the entities beyond the state control – there are no data on the volume and value of transactions made under this system. The providers of these services are not the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information. It is probable that the case of FT in the scope of the analysed scenarios will not be detected. Knowledge of the law enforcement authorities on the Hawala operations stems primarily from the operational knowledge and other foreign services. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3

Justification for the level of threat	The Hawala system is a type of an informal banking system. It is used among others in the international trading, frequently to transfer funds to great distances. The important component thereof is the opportunity to ensure full anonymity and using several intermediaries when ordering a transfer. A person depositing cash is not asked to present any identity document and is usually unknown or poorly known to a given intermediary. Similarly, a withdrawing person may collect the delivered funds only by providing the agreed password. In this manner, an entity offering services in the Hawala system usually does not know from whom, for what and to whom it transfers funds. The key issue is the trust between the intermediaries, who are in most cases the members of a single family, friends, or recommended persons, and operate in a few or several countries. The fact that the persons depositing and withdrawing cash do not need to hold a bank account in a given country is also of importance (in many cases, due to restrictive local banking provisions, they cannot open the account in this country). The volume of payments/trading made via such informal systems remains unknown. There are no numerous ethnical minorities in Poland, in which the Hawala systems are common (however a continuously growing number of the foreigners from the higher risk countries staying in the Republic of Poland has been observed). One should also take into account the presence of a large number of Ukrainian refugees in Poland, which for the single fighters, who have been previously operating in Syria and Iraq in various groups associated with the Islamic State and the fighters from the Caucasus Emirate, has been the country, where they could obtain the necessary documents and then – via Poland – move to Western Europe. In the era of the military conflict in Ukraine, such migration of fighters is potentially facilitated. The Polish services have already observed in their operations the cases of using this method to transfer funds for the purposes of terrorist activity. CONCLUSION: The level of threat associated with the use of the informal Hawala banking system for transferring assets for the purposes of terrorist activity poses a high threat of terrorism financing.

The regulatory basis for the European payment services market is the[21] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (PSD). This Directive aimed primarily at opening the financial market to the new entities to enable providing payment services listed in the Annex to this Directive to other entities than the banks, by means of covering these entities with prudential supervision and provide the users benefiting from the services of these entities with adequate protection. Before enacting the PSD, the activity in the area of payment service could be conducted under the principle of freedom to conduct business. However, considering the accompanying risks, the PSD introduced the requirement of obtaining the authorisation for providing the services by the payment institutions and the opportunity – under certain conditions – to conduct the activity in the area of payment services in a limited scope without the need to obtain the authorisation and only on the basis of entry into the register kept by the competent supervisory authority (in Poland – the Polish Financial Supervision Authority) and legal framework for providing payment services by their providers.

The provisions of PSD were transposed to the Polish legal systems by the *Act of 19 August 2011 on payment services*. The provisions of this Act implemented the rule that the payment services can be provided only by the payment service providers, that is - apart from the banks – also by among others the payment institutions, electronic money institutions and payment service bureaus. This means that providing payment services, if not provided by any of the authorised entities (for example by the banks

[21] Source: https://www.knf.gov.pl/dla_rynku/procesy_licencyjne/platniczy/informacje_ogolne/zakres_uslug_platniczych, access: on 12.12 2022

on the basis of relevant provisions of the statue), requires the authorisation from the Polish Financial Supervision Authority for conducting the business as a national payment institution, small payment institution or entry into the register of payment services as a payment service bureau.

There is no definition of payment services. There is only the exhausted list of specific types of activities that should be considered the payment services. The payment services are understood as the activity consisting in[22]:

1) accepting cash deposits and making cash withdrawals from the payment account and all activities necessary to keep the account;
2) execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider through:

    a) direct debits, including one-off direct debits,
    b) a payment card or a similar device,
    c) credit transfers, including standing orders;

3) execution of payment transactions listed in clause 2 above, against funds made available to the user under the credit, and in the case of a payment institution or electronic money institution – a credit referred to in Article 74(3) *of the Act on payment services* or Article 132j(3) of the Act on payment services;
4) issuing of payment instruments;
5) enabling the execution of payment transactions, originated by the merchant or by the intermediation of the merchant, through a payment instrument of a payer, in particular on authorisation handling, sending to the issuer of a payment card or payment order execution systems of the payer or merchant, aimed at transferring to the merchant of due funds, excluding the activities consisting in accounting and settlement under the payment system in the meaning of the Act on settlement finality (acquiring);
6) providing the money transfer service;
7) execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the payee.

The Polish Financial Supervision Authority keeps the registered called the ERUP 2 KNF System[23], to which the national payment institutions, small payment institutions, payment service bureaus, cooperative savings and credit unions, the National Association of Cooperative Savings and Credit Union, national electronic money institutions and branches of the foreign electronic money institutions are entered. The register is open and accessible to third parties via the official Polish Financial Supervision Authority website.

The Hawala system is based on the network of intermediaries called the hawaladars or the Hawala banks, usually operating unofficially under the cover of another business activity. The Hawala intermediary runs *de facto* an underground bank, granting loans, accepting the deposits and executing transfers throughout the world, practically outside the official banking system, using one-off passwords. The core feature of the Hawala system is the swiftness of transfers, anonymity, possibility to transfer practically any amount, no formalities or documents and being absolutely invisible for the official banking system. The economics, reliability and avoiding taxation are also of importance. The Hawala transactions are

[22]Ibidem
[23]https://e-rup.knf.gov.pl/index.html

made immediately upon accepting cash by the intermediary and providing the password. The intermediary, when accepting cash from the depositing person, immediately orders – through fax, e-mail, phone call, chat, entry in social media, advertisements on the Internet, or any other manner that raises no suspicions, the withdrawal of cash to the authorised person in the other state. The entire transaction is based on trust between the intermediaries. The important element of informal banking system is the possibility of maintaining full anonymity, both of the depositing and withdrawing persons and using several intermediaries when ordering the transfer. In this way, the Hawala system operator usually is unaware from whom, for what and to whom it makes a transaction.

Vulnerability of the sector

All entities being the payment service providers offering money transfer services (excluding the payment institutions from the other EU Member States providing payment services at the territory of Poland by means of the agents) are the obligated institutions (OIs). Although these entities apply customer due diligence measures, the controls continue to reveal the deficiencies in this area. Customer due diligence measures provided for the Act include in particular the measures related to identification of customer and verification of its identity; identification of a beneficial owner and taking reasonable measures to verify its identity and determine the ownership and control structure in the case of a customer being a legal person or an organisational unit without legal personality. In addition the payment service entities should assess the business relationships of the customer and (as appropriate) obtain information on their purpose and intended nature. They should also monitor the business relationships of their customers on the on-going basis. However, according to acquired information, the operation of small payment institutions and payment service bureaus involves certain difficulties related to actual monitoring of transactions of their customers. The payment institution sector entities are aware of their AML/CFT obligations. In the area of non-banking money transfers in 2019-2021, the General Inspector of Financial Information (GIFI) received and executed 28 suspicious transactions reports. In 2019, these accounted for approx. 2.3% of all investigations on the suspected money laundering or terrorism financing in connection with the use of non-banking money transfers for suspicious transactions, in 2020 for approx. 0.9% and in 2021 for approx. 1.5%.

One should note that the payment services sector development is highly dynamic, with accompanying introduction of the innovative technologies and new, increasingly complex payment services, overpassing the technical capacities of certain payment schemes and systems. With regard to the above, the payment services market faces significant problems with due fulfilment of the obligations provided for in the Regulation 2015/847 on the transfers of funds transmitted through may payment service providers and multi-level structures of transfer handling. This refers in particular to the transfers executed in the payment chain by the banking and non-banking payment service providers. In such situations, during the execution of transfer, there are many cases of obfuscation or distortion of data of actual payers and payees in the payment chain and in some cases these data are not provided by the payment service provider of the payer at all. Considering the above, the combined supervisory authorities, i.e.: the European Banking Authority – EBA, the European Securities and Markets Authority - ESMA and the European Insurance and Occupational Pensions Authority – EIOPA issued, under Article 25 of the Regulation 2015/847, the common guidelines on the measures to be taken by the payment service providers to detect missing or incomplete information on the payer or payee and the procedures to be implemented to manage the transfer of funds, for which the required information is mission. According to the Office of the Polish Financial Supervision Authority (PFSA) – failure to comply with the requirements of the Regulation 2015/847 affects the security of the payment system and generates additional risk of using this system for the purposes of criminal activity, including money

laundering and terrorism financing. This affects also the capability of implementing the special mitigating measures against the persons and entities referred to in Article 118(1) *of the Act on counteracting money laundering and financing of terrorism.*

According to the General Inspector of Financial Information (GIFI) information, the payment services sector institutions – payment service providers should (following the Office of the PFSA recommendations – analyse data on transactions and direct debits and have implemented tools for event logs assessment. Due to the costs of maintaining the state-of-the-art dedicated IT tools, not all payment services sector institutions hold such state-of-the-art automated IT tools and systems supporting the delivery of the objectives of counteracting money laundering and financing of terrorism.

In order to raise the AML/CFT awareness in the obligated institutions – including in the payment institution sector, the GIFI has carried out trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of customers as well as reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) were provided. The trainings in the other AML/CFT aspects, organised both by the GIFI and by the PFSA under the CEDUR Programme, were also carried out.

Due to pending military conflict in Ukraine, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons. The existing language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. Considering the growing business activity of the entities providing payment services in the territory of Poland, one should point out at low number of reports submitted by these entities to the GIFI. In addition, with regard to the operation of the foreign payment institutions in Poland, accounts of which are kept by the national banks – there is a risk that the national banks have no sufficient information on the serviced foreign entities. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU states, in particular as regards the entities of complicated capital structure. In addition, the activity of payment institutions both as the entities involved in money laundering and used for the purposes of money laundering by their customers, consists in the operation of these payment activities in the scope of opening of multiple payment accounts for the foreign entities. This is associated with the increasing phenomenon of opening accounts on the basis of fictitious documents, used primarily for the purposes of laundering of the proceeds of crime, commonly called the "frauds". In addition, the payment institutions are established only for the purpose of transferring the proceeds of crime.

Online transfer services are relatively easily available – all you need is access to the Internet. There are possibilities to hide the identification data of a person using this type of payment services (with regard to COVID-19, many institutions enabled the transactions made to a specific amount without verification of identification data, while verification of identification data itself is simplified – based on the scan or a passport or driving licence provided by the customer, photo from an online camera and geo-location data of the customer). Transfers of funds are frequently of international nature. Innovative payment instruments and services, such as Google Pay, Apple Pay, Revolut and other continue to gain on importance on the Polish market. Only a part of these service providers is the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of ML or FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

With a view to the legislation in the area of money transfer service it should be noted that Poland as the EU Member State directly applies the Regulation (EU) 2015/847 on information accompanying transfers of funds. This means that the payment service providers (as the obligated institutions) perform their services only when transfers of funds are accompanied with complete information on the payer (transfer originator), including its name, number of payment account, address, number of the official ID document, ID number of customer o a date or place of birth. They must be sure that the transfer of funds is accompanied with information on the payee (beneficiary), in particular the name of payee and its payment account number or, if transfer is not made from/or on the payment account, the unique ID of the transaction. Information on the payer and payee are stored by the payment service providers for the period of five years (with possible extension). In addition, Article 148 of the *Act on counteracting money laundering and financing of terrorism* sets out the administrative penalties for the obligated institutions, which fail to comply with the obligations to assure that the transfers of funds are accompanied with information on the payer or payee or to implement the effective procedures to detect whether information on the payer or payee is missing. The payment service providers must also implement the effective procedures, including, as appropriate, ex-post or real-time monitoring in order to detect whether information on the payer and the payee is missing. Each payment service provider must have the effective risk-based procedures in order to allow them to decide whether to execute, reject or suspend that transfer for which the required information on the payer and payee is missing, and to determine the appropriate follow-up action to take.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of analysed risk to a large extent.

The Hawala system services are provided by the entities beyond the state control. Therefore, there are no data on the volume and value of transactions made under this system in Poland. The providers of these services are not the OIs.

Due to absence of operational powers and of reporting of Hawala transactions by the entities, the General Inspector of Financial Information (GIFI) is not capable to collect and analyse information from the entities executing such transactions. It is probable that the case of ML or FT in the scope of the analysed risk will not be detected. Knowledge of the law enforcement authorities on the Hawala operations stems primarily from the operational knowledge and other foreign services. The Hawala services involve a large number of transactions of complex and cross-border nature, to which the AML/CFT supervision in the sector focused in accordance with the risk-based approach, does not apply. It is impossible to identify neither the financial audit trail nor monitor the transaction.

Threats in the sector

In terms of money laundering as well as terrorism financing threat assessment, the payment services sector (offered by the other entities than the banks) is frequently used in relation to predicate offences in the area of money laundering and terrorism financing: tax offences, drug trafficking, property and trading offences, corruption, human trafficking or frauds.

Both money laundering and terrorism financing through the products offered by the payment services sector (offered by the other entities than the banks) in the form of, for example, money transfers or online money transfers, belong to the simplest methods to be used. This is due to the available options of applying the simplified customer due diligence measures at low amounts of transactions by the money transfer service providers. This is of importance in particular for the potential terrorism financing transactions. Due to well-developed payment service system in Poland, this method is commonly

accessible, while its application is inexpensive. It requires also neither specialist knowledge nor skills. Particularly high risk of ML and FT is attributed to so called cascade structures, where the payment institutions service other payment institutions. Identification of the actual originating party and the beneficiary of the transaction is hindered or impossible. A particular focus in such cases should be on the payment institutions, which:

- are registered in Poland but are owned by the foreigners;
- are foreign, and outside holding the account(s) in Poland seem to have no other connections with Poland;
- are personally related with the other payment institutions (in the cases, in which a given person establishes the successive payment institutions – usually the payment service bureaus);
- provide the services, to which they are not authorised to or exceeding the turnover thresholds for a given category of institution.

In addition, due to the relatively low amounts of transfers of funds, these transfers can be not recorded in the system as suspicious and – additionally – are easy to apply, however require planning and knowledge.

For the Hawala system, the important component of this informal banking system is the opportunity to ensure full anonymity and using several intermediaries when ordering a transfer. A person depositing cash is not asked to present any identity document and is usually unknown or poorly known to a given intermediary. Similarly, a withdrawing person may collect the delivered funds only by providing the agreed password. One should note that the Polish law enforcement authorities have already recorded the cases of using the Hawala system as the method for transferring funds intended both for the purposes of money laundering and potentially for terrorist activity in their operational activities.

In context of threats related to the potential terrorism financing, the conflict in Ukraine generates the threat to Poland related to penetration by one of the pan-Islamic and fundamentalist organisations of international range through the eastern border and potential operation in the country. This organisation opts for reinstitution of caliphate covering the entire Muslim world. The units of such organisation have also occurred in Poland, while the propaganda is addressed to the converts, migrants from the Middle East North Africa (MENA) area and the Chechens. It is highly probable, that there can be supporters of this organisation among the Ukrainian or Russian refugees, the more that before the annexation of the Crimea by Russia, this organisation has been operating there legally. This organisation has been also operating legally in several western countries, while in the United Kingdom and Germany it was banned. The financial flows involving the members of supporters of this organisation may be associated with terrorism financing.

Averaged level of threat of the payment services sector – ML – 2.33 and FT – 3.67

Averaged level of vulnerability of the payment services sector – ML – 3.0 and FT – 3.33

Estimated level of probability for the sector – ML – 2.73 and FT – 3.47

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML

and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the payment services sector –2.68	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the payment services sector – 2.64	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the payment services sector (offered by the other entities than the banks) for the purposes of terrorism financing in Poland is at a high level.

CONCLUSION 2: The level of risk of using the payment services sector (offered by the other entities than the banks) for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the payment services sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The payment services sector entities should continue their activities related to appropriate assessment of the business relationships of the customer and obtaining information on their purpose and intended nature as well as to strengthen on-going monitoring of business relationships.

The payment services sector should undertake the actions enhancing the awareness of exposure to the crime of money laundering and terrorism financing, as well as increasing the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

Continued development by the payment services sector institutions of the advanced IT systems and tools supporting the delivery of the objectives of anti-money laundering and counter-terrorism financing and implementation of such solutions by the entities which have not used them yet is recommended.

The trainings for the obligated institutions from the payment services sector, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be continued. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The Obligated Institutions keeping the payment accounts should put particular attention to the transfers of funds to the jurisdictions of higher risk of money laundering and terrorism financing. The focus should be in particular on cyclical transfers of funds with an enigmatic title of a payment order or repeating transfers of funds to a specific jurisdiction, without any business justification fo such transfers. The obligated institutions should place particular emphasis to determination of data on the source of origin of transferred assets as well as documents justifying the specific transaction.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance.

The obligated institutions should put particular attention to the basis of execution of a specific transaction, especially in order to confirm that the transactions are compliant with knowledge of the obligation institution on the customer.

If the obligated institution customer uses the solutions enabling payments via payment terminals o applications used for execution of payments, the factor considered by the obligation institutions should be the circumstances pointing out at disproportionately high value of transaction as regards the profile of business activity of the customer or as regards to already collected information on the customer.

The risk mitigating measure for the payment services sector entities is the obligation to register the entity in the adequate register and supervisory activities of the Polish Financial Supervision Authority.

3. Area – insurances

Sector description - is contained in sub-chapter 2.1.2. of NRA "Financial market sectors" and in chapter 6.3. "The most common methods used to finance terrorism".

Risk occurrence scenarios (i.e. possible risk occurrence examples) both for money laundering and terrorism financing – referred to the use of financial products and services in the form of life insurance policy and with regard to terrorism financing also the motor insurance policies for money laundering and terrorism financing purposes. Their description is presented below.

Money laundering

Table 15

Type of used services, financial products	Life insurances
General risk description	Using the possibilities offered by life insurances linked to investment fund
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The illicit proceeds are allocated by the offenders in life and endowment insurances or life insurances linked to investment funds purchased for own purposes or for the closed relatives, as additional contributions. After a certain time, the funds from these contributions are withdrawn and transferred further on a bank account of an offender or a person controlled by it. 2. Purchasing an insurance policy with additional options, for example, possibility of partial surrender of the policy, withdrawal of paid contributions, possibility of transferring funds on the policy account by third persons. This method enables making transactions outside a typical bank account, for example when avoiding the bank account enforcement.
Level of vulnerability	2
Justification for the level of vulnerability	Purchasing life/endowment insurances is relatively easy. It is difficult to hide the identification data of the insured or the beneficiary. There is a possibility to execute transactions of international nature, if the customer of a Polish insurance company is a resident of another country or makes a financial transaction through a foreign account. All these service providers are the OIs. These entities have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk.
Level of threat	2
Justification for the level of threat	Using the opportunities offered by life insurances linked to investment funds to legitimise the proceeds of crime is one of the identified money laundering methods. Although the GIFI has received information from the obligated institutions and cooperating units on using such *modus operandi*, this method is perceived as unattractive and relatively unsafe. This *modus operandi* requires planning, knowledge and skills to apply it. It requires preparing and updating documentation for insurance purposes. This is also an expensive method. CONCLUSION: Using the opportunities offered by life insurances linked to investment fund to legitimise the proceeds of crime poses a medium threat of money laundering.

Terrorism financing

Table 16

Type of used services, financial products	Motor insurances
General risk description	Insurance claim frauds for the purposes of terrorism financing
Risk occurrence scenario (i.e. possible risk occurrence example)	Causing a deliberate vehicle crash for the purposes of receiving compensation. which will be allocated for terrorism financing.
Level of vulnerability	4
Justification for the level of vulnerability	Obtaining a motor insurance is relatively easy. It is difficult to hide the identification data of the insured or the beneficiary. There is a possibility to execute transactions of international nature, if the customer of a Polish insurance company is a resident of another country or makes a financial transaction through a foreign account. All these service providers are the OIs. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information on this type of services. It is probable that the case of terrorism financing in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation do not correspond to the scope of the analysed risk to a large extent.
Level of threat	1
Justification for the level of threat	Using the insurance claim fraud scheme may be one of the forms of terrorism financing. However the level of complexity of the compensation procedure, preparation of adequate documentation and the risk of contacts with law enforcement authorities makes this method of financing the terrorist activity unattractive. In Polish conditions, there is no clear information on using this *modus operandi* to finance the terrorism. It is difficult to apply due to the need of holding specialist knowledge in presence of cheaper and easier methods of financing the terrorist activity. CONCLUSION: Using the insurance claim fraud scheme to collect funds for financing the terrorist activity poses a low threat of terrorism financing.

Table 17

Type of used services, financial products	Life insurances
General risk description	Allocation of money from policy for the purposes of terrorism financing
Risk occurrence scenario (i.e. possible risk occurrence example)	Cancellation of life insurance policy to obtain money from the previously paid contributions before the movement of the foreign terrorist fighters to the conflict zone.
Level of vulnerability	2

Justification for the level of vulnerability	Purchasing life/endowment insurances is relatively easy. It is difficult to hide the identification data of the insured or the beneficiary. There is a possibility to execute transactions of international nature, if the customer of a Polish insurance company is a resident of another country or makes a financial transaction through a foreign account. All these service providers are the OIs. These entities have certain awareness of their AML/CFT obligations, although relatively few information on suspicious transactions/activity is reported by life insurance companies. One should not however that with regard to the COVID-19 pandemic, the insurers have adjusted their sales system to the actual economic conditions and – in order to maintain the level of sales of life insurance contracts – deployed the technological solutions enabling distant access to insurance contracts. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of terrorism financing in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The insurance companies established the internal structures to detect frauds. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk.
Level of threat	1
Justification for the level of threat	Using the funds from a cancelled life insurance policy can be one of the forms of terrorism financing. However, this *modus operandi* may be relatively expensive due to the possibility of losing a part of funds (related to the terms and conditions of an insurance contract), which makes the attractiveness of this form of financing the terrorist activity relatively low. Poland, where there have been a relatively low amount of recorded cases of movements of terrorist fighters to the conflict zone, has no clear information on the use of this *modus operandi* to finance the terrorism. There are less expensive and easier methods of financing the terrorist activity. CONCLUSION: Using the funds from a cancelled life insurance policy to finance the terrorist activity, in particular the movement of the fighters to the conflict zone, poses a low treat of terrorism financing.

According to the Insurance Europe report, the largest European insurance market in 2020 was the United Kingdom[24], followed by France and Germany. As of the end of 2021, the total value of assets of the national insurance undertakings amounted to PLN 201.6 billion. In order to assess the size of the Polish insurance market, one should be aware that the total value of the collected insurance contributions in 2021 amounted to PLN 69.2 billion[25], of which life insurances accounted for 32%, while property insurances for approx. 68%. The total value of compensations and benefits amounted to PLN 41.3 billion in 2021. Compensations and benefits in the individual groups (Section I) amounted to PLN 18.4 billion, including life insurance benefits of PLN 7.5 billion, motor liability insurances of PLN 9.3 billion and comprehensive motor insurance (Autocasco) of PLN 6.0 billion. The number of policies of the remaining personal and property insurances (excluding civil liability insurances of the owners of motor vehicles and comprehensive motor insurance (Autocasco) policies) as of the end of 2021 amounted to 58,135,637. The share of bancassurance (the form of services exchange between the bank and insurance undertaking, consisting in mutual offering of the insurance products to the customers of the bank and banking products to the customers of insurance undertaking) in the life insurance contribution is 19.0%.

[24] Report of the Polish Chamber of Insurance "Ubezpieczenia w liczbach 2021 Rynek ubezpieczeń w Polsce"
[25] Ibidem

The value of life insurance contribution reached PLN 4.2 billion, while the value of property insurance contribution is PLN 2.6 billion.

In the life insurance segment, the payments from life insurance policies amounted – after three quarters of 2022 – to PLN 14.5 billion, of which PLN 5.1 billion were the payments from the protection life insurance policies. This amount was by 8% lower compared to the same period in the previous year. In 2022, the insurance undertakings have been recording lower mortality rates compared to the previous year, which translates into the observed drop in payments in this market segment. As of the end of 3Q of 2022, total revenue from life insurance contributions amounted to PLN 15.9 billion, of which as many as PLN 12.7 billion (increase by 5.1%) was assigned to the protection life insurances (PLN 7.1 billion) as well as accident and sickness insurances (PLN 5.6 billion).

According to data of the Polish Chamber of Insurance[26], in 2021 there were more than 25 thousand cases of claim frauds in Poland. More than 4.5 thousand cases covered life insurances, while vast majority – nearly 21 thousand – the property insurances. Undue payments for the amount of nearly PLN 442 million were prevented – PLN 34 million in life insurances and PLN 408 million in property insurances. The frauds covered not only property, but also personal damages having a significant impact on the amount of undue benefits. In life insurances, similarly as in 2020, the most frequent cases included hospital treatment and surgeries. This accounts for more than 50% of all section I insurance frauds. 18% are the cases related to permanent disability or health injuries in effect of an accident. Similarly as in 2020, the number of false submissions related to death of the insured, both in terms of numbers and amount of prevented payments.

The activity of insurance undertakings in Poland is supervised by the Polish Financial Supervision Authority. The register of insurance intermediaries is available on the PFSA websites. The register of insurance intermediaries consists of the register of agents and register of brokers.

Vulnerability of the sector

All insurance service providers are the OIs. They are aware of their AML/CFT obligations, although relatively few information on suspicious transactions/activity is reported by life insurance companies. In terms of insurance policies, in 2019-2021 the General Inspector of Financial Information (GIFI) received and handled only 4 suspicious transaction reports. Statistically, the number of insurance policy-related cases executed by the GIFI in 2019 accounted for only approx. 0.2% of all investigations on the suspected money laundering or terrorism financing in context of using the insurance policies for suspicious transactions, in 2020 for approx. 0.2%, while in 2021 for approx. 0.4%. Although the insurance sector entities apply customer due diligence measures, referred to in the Act, the controls continue to reveal the deficiencies in this area. Customer due diligence measures referred to in the Act cover in particular the activities related to identification of the customer and verification of its identity; identification of beneficial owner and taking reasonable measures to verify its identity and determine the ownership and control structure in the case of a customer being a legal person or an organisational unit without legal personality. In addition, the insurance service providers should assess the business relationships of the customer and (as appropriate) obtain information on their purpose and intended nature. They should also monitor the business relationships of their customers on the on-going basis. One should not however that with regard to the COVID-19 pandemic, the insurers have adjusted their sales system to the actual economic conditions, meeting the anti-money laundering and counter-terrorism financing requirements in order to maintain the level of sales of life insurance contracts. This involved in particular deploying of technological solutions enabling distant access to insurance

[26] https://piu.org.pl/analiza-przestepczosc-ubezpieczeniowa-w-2021-r/, access on 13.12.2022

contracts. The insurance sector is affected by the external factors i.e. COVID-19 pandemic and the outbreak of war in Ukraine. In the opinion of insurance market, these factors significantly affect the existing level of risk related to conducting the insurance activity, in particular in context of proper use by the supervised entities of enhanced customer due diligence, including the measures related to the links of the customers of insurance undertakings of personal, capital or business nature with the entities from the Russian Federation or Republic of Belarus. At present, the insurance undertakings need to monitor the business relations with the customers or verify the beneficial owners in the insurance contracts to a significantly larger extent. According to information held by the GIFI, the banking sector institutions hold the advanced tools and IT systems supporting the implementation of the objectives of anti-money laundering and counter-terrorism financing. To this end, these institutions use for example the systems supporting the transaction process analysis or the systems dedicated to customer verification with a view to the sanctions lists. In addition, the GIFI has carried out trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of customers as well as reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) were provided. The trainings raising the AML/CFT awareness in the obligated institutions are also carried out. These trainings are organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme.

The intensity and level of detail of customer due diligence measures applied by the insurance undertaking, the form and scope of their individual use and modification of their detailed rules of implementation depend on the dedicated analysis of customer due diligence (CDD – refers to monitoring of customers and their activity to ensure that the customer has not changed significantly in time), aimed at reducing the possibility of making transactions at risk from the AML and CFT perspective. In such cases, it is necessary to correctly determine the identify and status of the parties of life insurance contracts, including the beneficiary and, as appropriate, the beneficial owner(s), specify the scope of control to be performed, in particular when the politically exposed person (PEP) is potentially involved.

In context of proper application of customer due diligence measures and due to pending military conflict in Ukraine, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons. The existing language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. Considering large number of personal and property insurance policies,

Considering a large number of personal and property insurance policies in Poland, a low number of reports submitted by these insurance entities to the GIFI should be emphasized. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU Member States, in particular as regards the entities of complicated capital structure.

The public administration authorities have knowledge on the money laundering and terrorism financing (ML/FT) risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of ML and FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. It should be noted, the insurance undertakings have implemented the professional structures aimed at detection and countering the insurance frauds.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

Although in terms of products the life insurance sector is potentially less exposed to the ML and FT risk compared to, for example, the banking sector, even in the case of relatively inflexible life insurance products there is a risk that the funds used for purchasing life insurances may be the proceeds of crime. There is also a relatively limited risk that the funds withdrawn from life insurance contracts could be used for terrorism financing purposes. When speaking about the insurance products, the focus should be on their sales channels. For example, a large volume of sales of life insurance products is usually executed through the agents, in the case of which the life insurer will have a limited contact with a policy holder or no such contact at all. Also certain features of the insurance products, presence of which in the offer may pose the increased ML and FT threat, are of importance. This involves the products designed in a way to store the funds or property of the insured, the products with potentially large number of investment accounts, the products offering the option of reposition of assets to a policy.

From the perspective of ML and FT threats, the increased threat may also result in a rapid expansion of the insurer's customer base or rotation of this base, especially if this is not associated with advertising campaigns run at that time. Another threat is the customers, non-transparent ownership or management structure of which makes them difficult to identify with a view to a beneficial owner of the insured or beneficiary.

The threat may be also correlated with the methods of payment for the insurance products. These involve cash or other forms of payment promoting anonymity, payments from different bank accounts held by unrelated third parties. The threat may be also posed by non-transparent or suspicious sources of origin of the investment funds, which are allocated to business relationships (for example purchasing a product with a large investment share by a low income person without the specified source of origin of the funds). In addition, higher threat may be posed by the products enabling earlier withdrawal from the investment and having the pre-defined surrender value. From the objective perspective, the ML and FT threats may be posed by the persons and entities – customers, beneficiaries, the insurer and/or related third parties, established in or associated with the countries of higher risk of money laundering or terrorism financing, or alternatively, living in the countries deemed reluctant to cooperate in the area of providing information on the beneficial owners.

There are also the areas in the insurance sector, in which using the insurance products causes a low threat and which demonstrate low vulnerability to money laundering and terrorism financing. The examples of such insurance sector areas of lower risk include the products paid only in the case of death and/or disability of the insured or insurance policies for the pension programmes, provided that there is no surrender clause and the policy cannot be used as a security. They include also the pension programmes guaranteeing the pension benefits to the employees, where the contributions are paid from the remuneration and the programme rules enable no assignment of the member share under the programme (for example low-value insurance contributions). Lower threat is also posed by servicing the customers being the public companies quoted on a stock exchange holding the appropriate disclosure requirements in order to ensure transparency of the beneficial ownership. No increased ML and FT threat is posed by the transactions covering the *de minimis* amounts, such as life insurance policies with the annual contribution not exceeding USD/EUR 1,000 or one-off contribution not exceeding USD/EUR 2,500.

Money laundering and terrorism financing through the products offered by the insurance sector is economically justified, however the level of complexity of the compensatory proceeding, preparation of

the relevant documentation and the risk of contact with law enforcement authorities makes this form of money laundering or terrorism financing relatively unattractive. Using of insurance products requires planning, knowledge and skills to apply. Using the insurance products requires preparation and updating the documentation for the purposes of insurances.

Averaged level of threat of the insurance sector – ML – 2.0 and FT – 1.0

Averaged level of vulnerability of the insurance sector – ML – 2.0 and FT – 3.0

Estimated level of probability for the sector – ML – 2.00 and FT – 2.20

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the insurance sector –1.92	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the insurance sector – 2.20	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the insurance services sector for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the insurance services sector for the purposes of money laundering in Poland is at a medium level.

Mitigation of the identified risks:

In order to mitigate the probability of using the insurance services sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating

measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The insurance services sector entities should continue their activities related to appropriate assessment of the business relationships of the customer and obtaining information on their purpose and intended nature as well as to maintain on-going monitoring of business relationships.

The trainings for the obligated institutions from the insurance services sector, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be continued. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The Obligated Institutions of the insurance services sector should put particular attention to the beneficiaries of insurance policies from the jurisdictions of higher risk of money laundering and terrorism financing. The focus should be in particular on the assignments of policies made with no justification of or such type of actions (in particular lack of factual personal or capital links between the assignor and the assignee).

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions (purchasing the policies or their assignments), is of particular importance.

4. Area – other financial institutions

Sector description - is contained in sub-chapter 2.1.2. of NRA “Financial market sectors” and in sub-chapter 7.2.1. “Vulnerability of the financial market”.

Risk occurrence scenarios (i.e. possible risk occurrence examples) both for money laundering and terrorism financing – referred to the use of financial products and services in the form of services on the Forex financial market, factoring, leasing, investment fund units as well as the securities accounts and dedicated cash accounts for money laundering and terrorism financing purposes. Their description is presented below.

Money laundering

Table 18

Type of used services, financial products	Services on the FOREX currency market
General risk description	Using a broker company operating on the Forex market as a "market maker" to legitimise the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. A company operating legally on the FOREX market as a broker and *market maker* is controlled by the persons linked to the offenders, who secretly finance its operations. The offenders open the accounts on the transaction platform administrated by this company. Thanks to confidential information and more favourable terms and conditions granted by this company, they multiply their capital, which is recognised before the tax office as profit from investments on the FOREX market. 2. Submission of unreliable/falsified factoring agreement to the bank in order to lend credibility of the executed transactions.
Level of vulnerability	2
Justification for the level of vulnerability	The services on the FOREX market are accessible via brokers. Hiding the identification date of the entity ordering the transactions on this market via a licensed broker is rather difficult. The transactions of international nature are possible only when the customer is a resident of the other country, or makes a financial transaction through a foreign account, or uses the services provided by a foreign entity. All brokerage service providers are the OIs (brokerage houses or banks having the brokerage offices in their structures) – however the customers may use the services offered via Internet by foreign entities. The OIs from this area have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed.[27] The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2

[27] During all controls performed in 2019-2020 by the PFSA (among others in 3 brokerage houses, in 2 investment company agents, in 1 bank performing the brokerage activity) the irregularities and non-compliance in the controlled areas were revealed, primarily in the scope of risk assessment and applying customer due diligence measures i.e. for example improper risk assessment in the area of brokerage services or incompliance of the operations of these activities with the applicable law.

Justification for the level of threat	Forex is the international foreign currency exchange market of a wholesale nature, under which the banks, large international corporations and the institutional investors from around the world perform the foreign currency exchange 24 hours a day using the telephone networks, IT connections and information systems. Using a legal, yet controlled by the offenders company operating on the FOREX market as a broker in the "market maker" model to legitimise the illicit proceeds, is an unattractive and relatively unsafe method. This *modus operandi* requires specialist knowledge on the foreign currency market, skills and planning. In the *market maker* model, the profits from share in the FOREX market recognised by the investor are the broker's loss. The broker cannot suffer losses continuously, because such losses raise suspicions. There is information on using this type of activity to commit predicate offences for the purposes of money laundering. CONCLUSION: Using a brokerage company operating on the FOREX market as a "market maker" to legitimise the illicit proceeds poses a medium threat of money laundering.

Table 19

Type of used services, financial products	Factoring
General risk description	Use of factoring to legitimise the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	A company operating on the Polish market (factoree), entered into a factoring agreement with 2 foreign entities (factor), under which it has paid for purchased goods. The funds crediting the accounts of the Polish company have originated among others from cash deposits made in the ATMs by the foreigners. The Polish company used to commit an offence was purchased by a foreigner as so called "shell" company to impede finding the actual heads of this criminal practice by the law enforcement authorities.
Level of vulnerability	2
Justification for the level of vulnerability	The factoring services in the form of buying-out by the factoring service provider of non-overdue receivables of the companies due from the counterparties for the goods and services have been applied on the financial market. Hiding the identification data of the entity ordering the transactions on this market is rather difficult. International transactions between the factoree and the factors are possible. An undertaking using the factoring service receives the funds from the transaction faster. All these service providers are the OIs. The entities operating in this area have certain awareness of their AML/CFT obligations. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.

Level of threat	2
Justification for the level of threat	Factoring is a service provided by the factor, which consists in the buying-out of invoices from the entity being the goods or service provider to its counterparties. The offenders can use a legally operating factoring company (controlled by them) to legitimate the illicit proceeds. This money laundering method is unattractive to the offenders. There is information on the use of this type of activity to commit the predicate offences for the purposes of money laundering. CONCLUSION: Using factoring to legitimise the illicit proceeds poses a medium threat of money laundering.

Table 20

Type of used services, financial products	Leasing
General risk description	Leasing transactions (similarly as in the case of factoring agreements) can be used to introduce the illicit proceeds into financial trading by the organised criminal groups
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Crediting the illicit proceeds to the account assigned to the leasing contract, followed by applying to the leasing company for reimbursement of overpaid funds. 2. Crediting the proceeds of crime by establishing a company – "shell company" (creating the appearances of a conducted business activity), followed by transferring the proceeds of crime to the account of the leasing company for the purposes of disbursement of loan for purchasing a vehicle.
Level of vulnerability	2
Justification for the level of vulnerability	Leasing transaction (similarly as in the case of factoring agreement) can be used for introduction of the proceeds of crime into financial trading. The decisive features include its complex nature (the offenders frequently use several ML/FT methods linked to a leasing transaction). These features are of importance, because the more complex and complicated the transaction, the easier it is to legalise in order hide the criminal origin of the funds. The financial leasing service providers are the OIs. The entities operating in this area have certain awareness of their AML/CFT obligations. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2

Justification for the level of threat	Using the opportunity of entering into a leasing contract and its repayment with the illicit proceeds is not perceived in Poland as an attractive money laundering method. There is few information on using this type of activity to commit predicate offences for money laundering. CONCLUSION: Using the leasing to legitimise the illicit proceeds poses a medium threat of money laundering.

Table 21

Type of used services, financial products	Investment fund units
General risk description	Purchase of units in the investment funds for the funds originating from illegal sources
Risk occurrence scenario (i.e. possible risk occurrence example)	The perpetrators have been regularly purchasing the units in the investment funds for small amounts to resell them upon accumulation and transfer the acquired funds abroad
Level of vulnerability	2
Justification for the level of vulnerability	Access to the units in the investment funds (IFs) is relatively easy. Hiding the identification data of the investment funds' customers is difficult. The international transactions related to purchase and sales of the units in the investment funds are possible only when the customer of a Polish IF is a resident of another country or makes a financial transaction through a foreign account or the units are purchased from a foreign IF. All these service providers are the OIs – however the customers may use the services offered by the foreign entities. The OIs from this area have certain awareness of their AML/CFT obligations, however certain deficiencies in their fulfilling continue to be revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2
Justification for the level of threat	Since the investment funds vary in terms of risk level and linked type of financial instrument, in which they allocate their assets, the obtained level of profit/loss on a purchased unit of fund can be different. These differences result also from time horizon of the investment and its purposes. The GIFI have had few information on investing the illicit proceeds in the investment funds. This always requires planning, skills and specialist knowledge on the financial market from the investor. *Modus operandi* of money laundering with the use of purchase of units in the investment funds for the illicit proceeds is perceived however as unattractive. CONCLUSION: Purchase of units in the investment funds for illicit proceeds poses a medium threat of money laundering.

Table 22

Type of used services, financial products	Securities accounts and dedicated cash accounts.
General risk description	Use of securities accounts and dedicated cash accounts for transferring and legitimising the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The perpetrators, through the companies established in particular in tax havens, allocate the illicit proceeds in the capital market. 2. The perpetrators use a cash account dedicated to the securities accounts, opened for a natural person or a linked company as the "distribution box". This account is used for transferring the illicit proceeds for their further transfer on the bank accounts of the other entities controlled by the offenders. 3. The securities account held by a person or an entity controlled by an offender is used for purchasing the securities for the illicit proceeds deposited on a cash account dedicated to this securities account and their re-sale in a relatively short timeframe. Any potential losses from these transactions are then the cost of legitimisation of these proceeds.
Level of vulnerability	2
Justification for the level of vulnerability	Opening of this type of accounts is relatively easy. Hiding the identification data of the customers is rather difficult. The transactions of international nature are present. All these service providers are the OIs. They have certain awareness of their AML/CFT obligations, however certain deficiencies in their fulfilling continue to be revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	The GIFI has certain information on using this *modus operandi* by the offenders. Payments on a cash account dedicated to the securities account, followed by various forms of investment operations with the use of these funds or withdrawal or transfer onto the other account simulates the legal origin of the assets obtained from the criminal activity. This is associated with the presumption that the funds deposited on the cash account dedicated to the securities account origin from the financial operations on a stock exchange. This *modus operandi* is perceived by the perpetrators as a relatively attractive form of money laundering. The level of complexity of the capital market acts as a solid advantage for the criminal activity aimed at money laundering. Although using the securities accounts and dedicated cash accounts to transfer and legitimate the proceeds requires specialist knowledge, skills and planning, the absence of top-class capital market experts in the law enforcement authorities makes this method relatively safe. CONCLUSION: Using the securities accounts and dedicated cash accounts for transferring and legitimating the illicit proceeds poses a high threat of money laundering.

Terrorism financing

Table 23

Type of used services, financial products	Services on the FOREX currency market
General risk description	Using a broker company operating on the FOREX market for fraud to obtain funds for terrorist activity
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The perpetrators register a company, which commences the activity as a broker company on the FOREX market without obtaining the applicable authorisation for the investment/brokerage activity. The company's offer is available in several languages and tempts with high profits. Thanks to this and using the aggressive marketing techniques, the company expands its base of customers, who make payments on the accounts of this entity to fund their brokerage accounts. The investors remain unaware that the transactions they made are fictitious and the funds will be appropriated by an illegal investment company at some point in time. In the case of the companies being so called market makers[28], there is also the option that they will be offered with less attractive terms compared with the market terms, in order to make them suffer losses, and the funds obtained in such way will be transmitted to the terrorist organisations. 2. The perpetrators register a company, which commences the activity as a broker company on the FOREX market without obtaining the applicable authorisation for the investment/brokerage activity. The supporters of terrorist organisations, who have transferred funds, make transactions, which are unprofitable to them (especially when the company operates as a market maker) or accept a steep commission or forfeiture of funds when such entity ends its operation. The funds obtained in this way are transferred to the terrorist organisations.
Level of vulnerability	2
Justification for the level of vulnerability	The services on the FOREX market are accessible via brokers. Hiding the identification date of the entity ordering the transactions on this market via a licensed broker is rather difficult. The transactions of international nature are possible only when the customer is a resident of the other country, or makes a financial transaction through a foreign account, or uses the services provided by a foreign entity. All brokerage service providers are the OIs (brokerage houses or banks having the brokerage offices in their structures) – however the customers may use the services offered via Internet by foreign entities. The OIs from this area have certain awareness of their AML/CFT obligations, although certain deficiencies in their fulfilling continue to be revealed. There is relatively few information on suspicious transactions/suspicious activity reported by the brokerage houses. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1

[28] An entity issuing and quoting the financial instruments and at the same time acts as the other party to the transactions made by the customer.

Justification for the level of threat	Forex is the international foreign currency exchange market of a wholesale nature, under which the banks, large international corporations and the institutional investors from around the world perform the foreign currency exchange 24 hours a day using the telephone networks, IT connections and information systems. Using a legal, yet holding no applicable authorisation for the investment/brokerage activity and controlled by the perpetrators company operating on the FOREX market as a broker in the market maker model, is an unattractive method of acquiring and transferring funds for terrorist activity. This *modus operandi* requires specialist knowledge on the foreign currency market, skills and planning. In the market maker model, the profits from share in the FOREX market (in effect of a fraud or wilful activity) are the broker's profit and can be transferred to the terrorist organisations. The GIFI has no information on any intent of using this *modus operandi.* CONCLUSION: Using a brokerage company operating on the FOREX market as a market maker for the purpose of fraud to obtain funds for terrorist activity poses a low threat of terrorism financing.

Table 24

Type of used services, financial products	Investment fund (IF) units
General risk description	Trading in units in the investment funds to collect funds for terrorist activity
Risk occurrence scenario (i.e. possible risk occurrence example)	T The perpetrators have been regularly purchasing the units in the investment funds for small amounts to resell them upon accumulation and transfer the acquired funds abroad.
Level of vulnerability	2
Justification for the level of vulnerability	Access to the units in the investment funds is relatively easy. Hiding the identification data of the investment funds' customers is difficult. The international transactions related to purchase and sales of the units in the investment funds are possible only when the customer of a Polish IF is a resident of another country or makes a financial transaction through a foreign account or the units are purchased from a foreign IF. There are however difficulties with verification of the foreign customers in the central registers of beneficial owners of the EU states, in particular as regards the entities of a complicated capital structure. There is relatively few information on suspicious transactions/activity reported by the investment fund associations and the IFs. All these service providers are the OIs – however the customers may use the services offered by the foreign entities. The OIs from this area have certain awareness of their AML/CFT obligations, however certain deficiencies in their fulfilling continue to be revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1
Justification for the level of threat	Purchase and trading in the units in the investment funds in order to collect funds for terrorist activity can be one of the *modi operandi* for terrorist financing. The

	GIFI has had however no information on investing the illegal or legal funds in the investment funds for this purpose. Trading in the units in the investment funds is a difficult to apply form of action due to the need to have specialist knowledge on the capital market, the more that there are less expensive and easier methods of terrorism financing. CONCLUSION: Using the purchase and trading in the units in the investment funds to collect funds for terrorist activity poses a low threat of terrorism financing.

Table 25

Type of used services, financial products	Securities accounts and dedicated cash accounts
General risk description	Using the securities accounts and dedicated cash accounts to collect funds for terrorist activity
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The perpetrators, through the companies established in particular in tax havens, allocate the illicit proceeds in the capital market. The purchased securities are then sold and the acquired funds are used for financing of terrorist activity. 2. The cash account dedicated to the securities account held by a foreign company controlled by the supporters of a terrorist organisation, is used for depositing funds from the bank account kept in the other country for a natural person under a fictitious title of investment in the shares of a public company. These funds are then – in a short time interval – transferred on a bank account kept in a third country, belonging to the company referred to above as a profit from trading in securities.
Level of vulnerability	2
Justification for the level of vulnerability	Opening of such accounts is relatively easy. Hiding the identification data of customers is rather difficult. There may be problems with verification of the foreign customers in the central registers of beneficial owners of the EU and non-EU states, in particular as regards the entities of complicated capital structure. The transactions of international nature are present. All these service providers are the OIs. They have certain awareness of their AML/CFT obligations, however certain deficiencies in their fulfilling continue to be revealed. There is relatively few information on suspicious transactions/activity reported by the brokerage houses. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1

Justification for the level of threat	Using the securities accounts and dedicated cash accounts to collect funds for terrorist activity can be one of the forms of terrorism financing. However, the level of complexity of the securities market makes this form of financing of terrorist activity unattractive. There is however no unambiguous information on applying this *modus operandi* for terrorism financing. It is difficult to apply due to the need to have specialist knowledge on the capital market, the more that there are less expensive and easier methods of financing the terrorist activity. CONCLUSION: Using the securities accounts and dedicated cash accounts to collect funds for terrorist activity poses a low threat of terrorism financing.

Pursuant to the Regulation of the European Parliament and of the Council (EU) no. 575/2013 and the Act of 27 August 1997 – Banking Law, the financial institutions are defined as the entities, scope of which covers:

- the undertakings, the principal activity of which is to pursue one or more of the activities: lending, leasing, payment services, issuing and administering the means of payment such as cheques, bills, certificates of deposit, foreign exchange, financial futures and options, swaps and securities), participation in securities, advice to undertakings on capital structure or industrial strategy and ownership transformations, money broking, investment portfolio management and advice, safekeeping and administration of securities and issuing electronic money;
- payment institutions and financial holding companies (excluding insurance holding companies);
- lending institutions operating under the Act of 12 May 2011 on the consumer loan.

Due to a relative diversity of services offered by the financial institutions listed above, this Annex to the National Risk Assessment in the financial institutions area lists the scenarios on services on the FOREX financial market, investment fund units and the securities accounts and dedicated cash accounts as the types of used services and financial products.

The Forex market is an international decentralised market, on which the participants (mostly banks, funds, insurance companies and other financial institutions) exchange one type of currency into another. Since the market offers not only the currencies of the largest global economies, Forex is the market of the highest liquidity in the world (i.e. approx. USD 5 trillion each day). In Polish practice of the Forex market, which has been developing dynamically for several years, its services are offered both by the national investment companies (brokerage houses or brokerage offices operating within the banks' structures) and by the licensed foreign entities operating primarily on a cross-border basis i.e. via Internet (this includes the foreign investment companies running the brokerage activity in Poland via its branch or on a cross-border basis – without the need of opening the branch, which are established at the territory of the European Union or the EEA and notified such activity or hold the applicable authorisation of the PFSA). These services have been associated with highly active and continuously developed promotional and marketing activities, aimed at acquisition of customers, who will commit their funds in the transactions on the Forex market. The phenomenon of increasing interest in the Forex market itself stems from the need of the investors to allocate the capital into the new financial forms, but primarily from the opportunity og generating much higher profits compared to the regulated market, which is associated with the Forex market (operations on the Forex market enable the use of so called financial leverage). Some companies offering the investments on the Forex market operate however illegally. A potential recipient of services on the Forex market should thoroughly verify who, and on what principles will intermediate in the transactions. The Polish Financial Supervision Authority (PFSA)

keeps a register – a list of public warnings – on its official website. It includes the financial market entities of doubtful activity, against which a notification of suspected offence was submitted.

The investment funds are primarily the form of collective investing. The investment fund is a legal person. Their tasks include investing of capital acquired from the investors. The funds are in most cases invested in the securities, financial market instruments and other property rights. The investment fund is available to a natural person, legal person and an entity without legal personality[29]. Joining the fund is associated with the need to place the order of purchase of units in the investment fund and a cash payment. The investment funds declare the financial instruments, in which they will invest, in their status. These instruments determine the potential profit to be generated by the fund and the risk associated with the investment in this fund. In terms of portfolio content criterion, the funds are divided into 4 groups:

- money funds (invest mostly in the money market papers, limited expected profit and risk),
- bond funds (invest mostly in bonds, expected profit and risk higher compared to the money funds),
- mixed funds (invest both in the shares and bonds, profit and risk usually higher compared to the bond funds),
- share funds (shares are the majority of the portfolio, the highest expected profit and risk).

The investment fund is established by the Investment Fund Company, being its authority, managing it and representing it in the relationships with any third persons. The consent for establishment of a public investment fund is issued by the Polish Financial Supervision Authority, which supervises its operation on a continuous basis. The investment funds in Poland are established and operate under the *Act on investment funds and management of alternative investment funds*, harmonised with the EU directives and concerning the collective investments in the transferable securities.

In terms of legal form criterion, the investment funds are divided into three categories: open-end investment funds, specialist investment funds and closed-end investment funds. The open-end investment funds may invest the assets in: securities, money market instruments, units in the investment funds, bank deposits. The Specialist Open-End Investment Fund is a form of an open-end fund. The offer of purchasing the units in such funds may be addressed to a specific audience, for example the institutions or participants of the pension programmes. The fund status may include the additional terms and conditions on buying back the units in the investment funds. The closed-end investment fund may incur credits and loans up to the amount of 75% of the fund's net asset value. Greater freedom in the formation of the investment strategy as well as no need to have a sufficiently high cash reserve balance enables the closed-end investment funds to establish differentiated investment strategies for effective use of the available funds, which generates potentially higher income compared to the open-end fund. As of the end of August 2022, there were 685 active investment funds managed by 64 Investment Fund Companies (IFCs)[30]. The total value of assets collected by the IFCs as of the end of June 2022 amounted to PLN 360.7 billion. The funds are subject to the obligation of entry into the register of investment funds. The register is kept by the District Court in Warsaw (register court).

The brokerage activity covers the performance of activities consisting in among others: accepting and transmitting the orders of purchase or sales of the financial instruments; purchasing or selling the financial instruments on own account; managing the portfolios encompassing one or more financial instruments; investment advice and offering the financial instruments. An investment company running the brokerage activity can be a brokerage house or a bank running a brokerage activity. A brokerage

[29] https://businessinsider.com.pl/poradnik-finansowy/oszczedzanie/jakie-sa-rodzaje-funduszy-inwestycyjnych/r0hfs9e, access on 11.01.2023
[30] https://www.gov.pl/web/finanse/fundusze-inwestycyjne, access on 13.01.1023

house can run the brokerage activity in the form of: a joint-stock company; a limited joint-stock partnership; a limited liability company; a limited partnership; a registered partnership. Performing the brokerage activity in Poland requires the authorisation of the Polish Financial Supervision Authority. The operation of the brokerage houses is strictly controlled by the Polish Financial Supervision Authority. An individual investor, who invests the funds through a brokerage office, is not a party to the transaction. Purchase and sales of securities on behalf of the customer are made by the brokerage house. The brokerage office customer holds a brokerage account being a type of an account used for keeping the securities and financial instruments and ordering their purchase and sales transactions on a stock exchange. IT is an electronic record kept by the authorised brokerage house or office for the customer, who may be a natural or legal person. The funds from transaction on the brokerage account can be withdrawn only onto the personal account combined with the investment account or any account defined as an additional transfer account. The statutory provisions require the brokerage houses to hire a sufficient staff under the employment contract (securities brokers and/or investment advisors). They define also the conditions to be met by the members of the management and supervisory boards and specify the mode of appointing of the president of the management board. The organisation associating the brokerage houses and offices in Poland is the Polish Chamber of the Brokerage Houses. As of the end of August 2022, 9 from among the total of 44 investment companies running a brokerage activity were the banks running a brokerage activity, while 35 the independent brokerage houses[31].

At the end of 2022, a significant change concerning the financial institutions involved in lending was introduced. The supervision of the Polish Financial Supervision Authority over the lending institutions[32] was introduced, with the options of imposing penalties on the member of a management board amounting to up to PLN 150 thousand and up to PLN 15 million on a lending institution, or deleting the lending institution from the register. This measure aims at countering the attempts of excessive, unjust enrichment at the cost of the consumers.

Vulnerability of the sector

Vast majority of the other financial institutions sector entities (with consideration to the definition provided for in the *Regulation of the European Parliament and of the Council (EU) no. 575/2013* and *the Act of 27 August 1997 – Banking Law*) are the obligated institutions (OIs). These entities are obliged to apply customer due diligence measures, set out in the Act of 1 March 2018 on counteracting money laundering and financing of terrorism, however the controls performed in this area reveal certain errors and deficiencies. Customer due diligence measures set out in the Act cover primarily the activities related to identification of the customer and verification of its identity; identification of beneficial owner and taking reasonable measures to verify its identity and determine the ownership and control structure in the case of a customer being a legal person or an organisational unit without legal personality. In addition, the other financial institutions sector entities should assess the business relationships of the customer and (as appropriate) obtain information on their purpose and intended nature. They should also monitor the business relationships of their customers on the on-going basis. Large obligated institutions of this sector, such as brokerage houses or investment fund companies are capable of performing the actually real-time monitoring of transactions made by their customers. The other financial institutions sector entities are aware of their AML/CFT obligations. In the scope of factoring service, capital market instruments, pre-paid cards, credits and loans (in the financial institution section), leasing – in 2019-

[31] https://www.gov.pl/web/finanse/domy-i-biura-maklerskie, access on 13.01.2023

[32] Covering the lending institutions with full-scope PFSA supervision in the meaning of the Act of 12 May 20211 on consumer credit, shall take place on 1 January 2024. At present, the PFSA performs no full-scope supervision over these institutions.

2021 the GIFI received and handled the total of 33 analytical cases on the suspected money laundering or terrorism financing related to the use of the institutions from the other financial institutions sector to execute the suspicious transactions, in 2020 of approx. 3.1%, and in 2021 of approx. 1.5%.

The other financial institutions sector entities are obliged to implement the effective procedures, including, as appropriate, for the ex-post or real-time monitoring in order to detect lack of information on the transaction parties or activities. Each entity in this sector must have defined the effective risk analysis-based procedures, which enable making the decision on whether to execute, reject or suspend a specific service or transaction, for which the required information on the activity or transaction parties is missing, or taking the appropriate further steps.

In effect of cooperation between the GIFI and the law enforcement authorities, the latter frequently use information stored in the GIFI databases (primarily financial information). Under Article 106(1) of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism, in the event of taking a suspicion on committing a tax offence or an offence other than money laundering or terrorism financing offence, the GIFI provides information justifying this suspicion to the competent authorities specified in Article 105(1) and (4) of this Act in order to take the measures resulting from their statutory tasks. In the event of taking a justified suspicion of an infringement of the provisions related to the financial market operation, the GIFI provides information justifying this suspicion to the PFSA.

The other financial institutions sector entities supervised by the PFSA should (following the Office of the PFSA recommendations) analyse data on the services and transactions and have implemented tools to assess the event logs. Due to the costs of having the state-of-the-art dedicated IT tools, not all institutions of the other financial institutions sector implemented such advanced automatic IT tools and systems supporting the implementation of the anti-money laundering and counter-terrorism financing objectives. The large obligated institutions of this sector of the greatest transaction number, such as the brokerage houses or investment fund companies, have implemented such systems.

In order to raise the AML/CFT awareness in the obligated institutions – including in the other financial institutions sector, the GIFI has carried out trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on anti-money laundering and counter-terrorism financing were provided. The training block concerning the determination of the beneficial owner and the ownership and control structure of customers as well as reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO), was an important training subject. The trainings in the other AML/CFT aspects for the sector entities were also carried out, both by the GIFI and by the PFSA under the CEDUR Programme

The other financial services sector institutions providing the services or making transactions in the form of the services on the Forex financial market, trading in the units in the investment funds and making transactions on the securities accounts and dedicated cash accounts are the licensed entities or the entities operating under the authorisations issued by the Polish Financial Supervision Authority.

The entities of the sector concerned may face problems with the acquisition of a broader spectrum of documents confirming the customer's identity or reliability. Due to the conflict in Ukraine and presence of large number of refugees in Poland, there are also serious problems with identification and verification of persons. The existing language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents.

A relatively low number of reports submitted by the other financial institutions sector entities to the GIFI draws attention.

In 2022, the GIFI performed the risk assessment scoring for the brokerage houses and offices for the period from the 1Q of 2019 to the 2Q of 2021 i.e. 6 reporting periods. Data on 30 brokerage offices and houses were analysed. The scoring covered the analysis with a view to such criteria as: share of low-risk customers in the total number of customers; share of PEPs in the total number of customers; share of beneficial owners of the PEP status in the general number of PEP customers. In terms of these criteria, seven brokerage offices and houses (from among 30) were considered as the institutions of high or medium-high risks. Six brokerage offices and houses were assessed as low-risk institutions, while the remaining seventeen brokerage offices and houses were classified with a view to the abovementioned criteria as the medium-risk institutions. A similar scoring was performed for the Investment Fund Companies. Data on 50 IFCs were analysed. The adopted risk assessment criteria for IFCs were identical as for the brokerage houses and offices. With a view to these criteria, seven IFCs (from among 50) were considered the institutions of high or medium-high risk. Fifteen assessed IFCs were considered as low-risk institutions, while the remaining twenty eight IFCs were classified with a view to the abovementioned criteria as the medium-risk institutions.

The public administration authorities have knowledge on the ML/FT risk in the scope of the sector concerned. The GIFI is capable to collect and analyse information. It is highly probable that the case of ML or FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

In terms of money laundering as well as terrorism financing threat assessment, the sector of services provided by the other financial institutions is the sector, which can be potentially used in relation to predicate offences in the area of money laundering and terrorism financing: tax offences, drug trafficking, property and trading offences, corruption, human trafficking or frauds. The level of capital and money markets complexity is a solid advantage for the criminal activity aimed primarily at money laundering. The law enforcement agencies employ few specialists having the most extensive knowledge and experience on these markets, while the swiftness of transactions on the capital and money markets and opportunity of multiple exchanges of funds into financial instruments at different exchange rates result in obfuscation of the transaction as a predicate office or money laundering offence in the event of the proceeds of crime.

Although the investments on the Forex market are legal, a significant increase in the number of offences using this market has been noticed. These offences consist primarily in fraudulent operation of the entities intermediating in the investments. The offenders frequently operate within the organised crime group[33]. There are many fraud variants. The perpetrators provide the investment advice, recommend the transactions on the Forex market via the investment platforms, and sometimes manage the customers' portfolios. Different scenarios of this type of frauds have certain common elements, which aim at encouraging the customers to make quick profits. These include asserting about the opportunities of quick and high profits on the Forex market; profit guarantee for "each customer"; "broker" support and the need to make the first payment (so called registration fee); the need to install an application (on a

[33] Information of the National Police Headquarters and FinCERT.pl – of the Banking Cybersecurity Centre of the Polish Bank Association (ZBP) on threat related to offers of the Forex market investments and crypto-currencies of 24.03 2021.

computer or phone), which enables automation of the Forex market operations; the need to send the scans (photos) of the ID document to the "broker", a selfie with a ID document or a valid bill to confirm the identity. The offenders may also inform that they will pay the return from the investment directly on the customer's card. Under this pretext, they ask to provide the card details. Stolen personal data are used to incur loans and credits, e.g. via Internet and sometimes the customer of an entity intermediating in the investments on the Forex market is unknowingly involved in criminal activity. During certain attacks, the offenders use the victim for laundering of the proceeds of crime (in transfer of funds from frauds at another victim):

- induce to transfer the invested funds onto the accounts of the other persons. This is supposed to facilitate further investments of the customers with regard to the alleged preventive measures taken by certain banks;
- for the same purpose, they agree with certain customers that their bank account will be credited with the funds from another person, which will be further transferred. In this way, the victim will be allegedly able to gain profit from its „investments" or make up for losses more easily.

Money laundering can also take place in particular when the broker is controlled by the offenders and the orders placed by the offenders or the substituted persons are executed. The financial operations on the Forex market financial instruments are then recognised as the profit from the investments on this market.

The securities may be transacted both under the organised trading and outside it. The securities market is a global market playing the key role in the global economy. Its participants include the multinational and multi-branch financial companies employing thousands of people on one hand and one-man offices offering the brokerage services or financial advice on the other hand.

Through the securities market sector (as well as the sector of investments in the investment fund units) the persons and entities may obtain access to the financial system, which creates the opportunity for the offenders to misuse this system. The offer of brokerage offices or investment companies addressed to this market contains and continues to develop the new products and services. These new products are triggered by the investors' demand, market conditions and dynamic technological progress. The complexity of the offered products affects the threat related to money laundering on this market. Some products and services are intended for sales to the general public, while the other are tailored to the needs of a single buyer. Transactions are in general made electronically and beyond the national borders. The features specific for the securities market, such as swiftness of transactions, global range and adaptation capacity, make this market attractive for the offenders, who use it for illicit purposes, including money laundering and terrorism financing. In addition, the securities sector is unique among the sectors, since it may be used both for laundering of the proceeds of crime committed somewhere else and to commit predicate offences by means of fraudulent activities on the securities market. The transactions and techniques linked to money laundering on one hand and the predicate offences related to securities on the other hand are frequently hard to distinguish. In practice, the GIFI has certain information on using the securities accounts and dedicated cash accounts for money laundering by the perpetrators. For example, money laundering is correlated with a working assumption that the funds deposited on a cash account dedicated to a securities account originate from the financial operations on a stock exchange. Thus, all deposits made on the cash account dedicated to the securities account, followed by various forms of investment operations with the use of these funds or withdrawal or transfer on the other account, simulate the legal origin of the assets, which have been previously gained from criminal activity.

Investing in closed-end investment funds (CEIFs) is a major threat from the perspective of money laundering and terrorism financing – a holder of certificate in anonymous, is able to trade them without any knowledge of tax authorities or supervision authorities over the capital market. CEIFs can be used to purchase the interests, shares, real estates, while profits generated through CEIFs (with certain exceptions) are not taxable.

In terms of terrorism financing, the use of financial products and services in the form of services on the Forex market, investment fund units as well as the securities accounts and dedicated cash accounts for the purposes of terrorism financing, has certain common features consisting in that the *modi operandi* listed above required specialist knowledge on the currency or capital market as well as skills and planning. To date, the GIFI has had no concrete information on investing the illegal or legal funds in the investment funds for the purposes of terrorist financing in the other financial institutions sector. The level of complexity of the Forex and securities markets results in relatively low attractiveness of this form of terrorist activity financing.

Averaged level of threat of the other financial institutions sector – ML – 2.2 and FT – 1

Averaged level of vulnerability of the other financial institutions sector – ML – 2.0 and FT – 2

Estimated level of probability for the sector – ML – 2.08 and FT – 1.60

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the other financial institutions sector – 1.56	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the other financial institutions sector – 2.25	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High

3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the other financial institutions sector for the purposes of terrorism financing in Poland is at a low level.

CONCLUSION 2: The level of risk of using the other financial institutions sector for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the other financial institutions sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The other financial institutions sector entities should enhance their activities related to appropriate assessment of the business relationships of the customer and obtaining information on their purpose and intended nature as well as to maintain on-going monitoring of business relationships.

The other financial institutions sector should undertake the actions increasing the awareness of exposure to the crime of money laundering and terrorism financing, as well as increasing the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

The trainings for the obligated institutions from the other financial services sector, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be continued. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The obligated institutions from the other financial institutions sector should put particular attention to the transfers of funds to the jurisdictions of higher risk of money laundering and terrorism financing. The obligated institutions should place particular emphasis to determination of data on the source of origin of transferred assets as well as documents justifying the specific transaction.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance.

The entities providing the factoring services should put particular attention to verification of the source of origin of assets, which in the case of factoring service should cover verification of the basis for issuing the invoices by the customer of the obligated institution. On-going monitoring of the business relationships and verification of the source of origin of assets can also cover the analysis of business relationships between the customer and its counterparties.

Due to the nature of the activity conducted by the obligated institutions from the other financial institutions sector, obtaining knowledge on the nature of business relationships of the customers as well as the source of origin of the assets available to the customer is of the key importance.

5. Area – foreign currency exchange

Sector description - is contained in sub-chapter 2.1.2. of NRA "Financial market sectors" and in sub-chapter 7.2.1. "Vulnerability of the financial market".

Risk occurrence scenarios (i.e. possible risk occurrence examples) both for money laundering and terrorism financing – referred to the use of financial products in the form of cash currency exchange, exchange of money within a single currency and services of the non-cash currency exchange service providers for money laundering and terrorism financing purposes. Their description is presented below.

Money laundering

Table 26

Type of used services, financial products	Cash currency exchange
General risk description	Currency exchange to impede identification of the proceeds of crime
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using cash currency exchange in the exchange offices by the offenders to impede tracking the transfer of assets path to the law enforcement authorities. Using the "trusted" exchange offices, not reporting the suspicious transactions to the financial intelligence unit. 2. Exchange of collected illicit proceeds in the exchange offices into high denomination banknotes in the other currencies (commonly exchanged throughout the world, for example EUR) for the purposes of easier transport across the state borders.
Level of vulnerability	2
Justification for the level of vulnerability	Access to such services is relatively easy. There are available options of hiding the identification data of customers (these service providers execute primarily the bearer transactions. Identification of a customer and its verification on-site takes place at each case of applying the customer due diligence measures – for transactions equivalent to EUR 15,000 and above). The public administration authorities have basic knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on this type of services, however provided by the entities being the OIs or made available by a foreign financial intelligence unit. It is probable that the case of money laundering in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation partially corresponds to the scope of the analysed risk.
Level of threat	3
Justification for the level of threat	Using the currency exchange to impede identification of the proceeds of crime is one of the most commonly applied money laundering methods. This method is easy, widely accessible, relatively inexpensive and perceived by the perpetrators as rather attractive. The currency exchange transactions below the registration thresholds raise no suspicions, especially when the employees of, for example, the exchange office cooperate with the offenders. High turnover volume of the exchange offices enables hiding the exchange of the illicit proceeds among the legal transactions. The GIFI has received information on using this method for money laundering purposes, in particular in combination with the other methods. CONCLUSION: Using the currency exchange scheme to impede identification of the proceeds of crime poses a high threat of money laundering.

Table 27

Type of used services, financial products	Exchange of money within a single currency
General risk description	Exchange of low denomination banknotes into higher denomination banknotes
Risk occurrence scenario (i.e. possible risk occurrence example)	Exchange of EUR low denomination banknotes into the EUR 500 or 200 banknotes to reduce the volume of carried cash[34].
Level of vulnerability	2
Justification for the level of vulnerability	Access to such type of currency exchange services is hindered and dependent on holding the banknotes of this denomination by the OIs. Hiding the identification data of the person making the transaction is easy, especially when the individual transactions are executed in relatively low amounts. Transactions of international nature are impossible. All these service providers are the OIs. They are aware of their AML/CFT obligations. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk.
Level of threat	3
Justification for the level of threat	Using the scheme of exchanging the low denomination banknotes into higher denomination banknotes is one of the commonly applied money laundering methods. Such operations are made in the banks, exchange offices, but also in post offices. This method is widely available, its use is inexpensive and perceived by the perpetrators as attractive. However, the safety of this method requires planning and following the rule of executing low-value transactions. Exchange of crumpled, frequently dirty low-denomination banknotes may be easily noticed. In most cases, this method requires cooperation of the employees working in the institutions providing such services. The GIFI has received information on using this method for money laundering purposes. CONCLUSION: Using the scheme of exchanging the low denomination banknotes into higher denomination banknotes poses a high threat of money laundering.

Table 28

Type of used services, financial products	Non-cash currency exchange service providers
General risk description	Non-cash currency exchange combined with transfer of funds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using non-cash currency exchange by the offenders in so called online currency exchange platforms to impede tracking of the transfer of assets path to the law enforcement authorities. For example – the funds in PLN are transferred to a so called online currency exchange platform from the bank

[34] The European Central Bank discontinued the issue of EUR 500 banknote on 27 April 2019. The main reason behind discontinuing the issue of this banknote was the concerns that these banknotes have been frequently used in criminal activity. The 500 EUR banknote, such as the remaining denominations, has retained its value and is exchangeable in the national central banks without any restrictions.

	account kept in one institution with the order of exchange into USD and transferring onto the account kept in the other bank, however in reality held by a different entity than the ordering party. 2. Transfer of funds (the proceeds of crime) to the online currency exchange platform from the account of a natural person being a victim of unauthorised access to its account.
Level of vulnerability	3
Justification for the level of vulnerability	Access to the currency exchange services is very easy. Hiding the identification data of the person making the transaction is easy, especially when the individual transactions are executed in relatively low amounts. It is possible to execute the transactions of international nature, if such transactions are made at least partially as cashless transactions. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU states, which refers in particular to the entities of complicated capital structure. All these service providers are the OIs. They have certain knowledge on their AML/CFT obligations. There is relatively few information on suspicious transactions/activity reported by the entities involved in foreign currency exchange. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation partially corresponds to the scope of the analysed risk.
Level of threat	4
Justification for the level of threat	Using the scheme of non-cash currency exchange in so called online currency exchange platforms combined with transfer of funds to impede tracking the transfer of assets path to the law enforcement authorities is the identified method enabling money laundering. At present, the online currency exchange platforms are not regulated by law. They are neither subject to any act nor any authority, which would establish their scope of operation. The online currency exchange activity is not subject to the PFSA supervision. The PFSA supervision applies only to providing the payment services with respect to such activity, which requires obtaining the relevant authorisations. According to the estimates presented in the Accenture report[35], the estimated volume of trading on the currency market (excluding the inter-bank transactions and forward transactions) in 2019 in Poland reached nearly PLN 1 trillion. Within the next three years, the projected increase was of approx. PLN 86 billion. A noticeable drop in growth dynamics results from the economic crisis triggered by the outbreak of COVID-19 pandemic. Non-cash currency exchange combined with transfer of funds is relatively inexpensive and as a *modus operandi* may be perceived by the perpetrators as an attractive and widely available method of money laundering. In the conditions of dynamic growth of economic trade in the export or import enterprises, non-cash currency exchange transactions in the online currency exchange platforms can be relatively invisible for the supervision (in particular in the absence of clear legal regulations). The GIFI has received very few information on the opportunities to use this method for money laundering purposes. Applying this *modus operandi* requires rather basic level of planning, knowledge and skills. It may be perceived by the perpetrators as relatively attractive and safe.

[35] Report: RYNEK WYMIANY WALUT W POLSCE, https://www.accenture.com ›_acnmedia › PDF-125

	The GIFI has received information on using this method for money laundering. CONCLUSION: Using the scheme of non-cash currency exchange in so called online currency exchange platforms combined with transfer of funds poses a very high threat of money laundering.

Terrorism financing

Table 29

Type of used services, financial products	Cash currency exchange
General risk description	Currency exchange to impede identification of the terrorism financing offence
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using cash currency exchange in the exchange offices (for example exchange from USD to USD) by the persons associated with the terrorist organisations to impede tracking the transfer of assets path to the law enforcement authorities. Using the "trusted" exchange offices, not reporting the suspicious transactions to the financial intelligence unit. 2. Exchange of collected funds (for example from the supporters) in the exchange offices into high denomination banknotes in the other currencies (commonly exchanged throughout the world, for example EUR) for the purposes of easier transport across the state borders.
Level of vulnerability	2
Justification for the level of vulnerability	Access to such services is very easy. Hiding the identification data of a person making the transaction is easy, especially when the individual transactions are made for the relatively low amounts. In many cases, proper identification and verification of the identity of the Ukrainian refugees is hindered. All these service providers are the OIs. They are aware of their AML/CFT obligations. There is relatively few information on suspicious transactions/activity reported by the entities involved in foreign currency exchange[36]. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk.
Level of threat	2

[36] Excluding the banks providing the currency exchange service, including online.

Justification for the level of threat	Using the currency exchange to impede identification of the terrorism financing offence is relatively easy and widely available. It is relatively inexpensive and perceived by the perpetrators as rather attractive, especially that the funds can origin from fully legal sources. The currency exchange transactions below the registration thresholds usually raise no suspicions. High turnover volume of the exchange offices enables hiding the exchange of the illegal or legal proceeds among the legal transactions. There is no information on running the exchange offices by the entities associated with the individuals suspected of terrorism or by the FTF. The GIFI has received very few information on using this method for terrorism financing purposes. CONCLUSION: Using the currency exchange scheme to impede identification of the terrorist financing offence poses a medium threat of terrorism financing.

Table 30

Type of used services, financial products	Exchange of money within a single currency
General risk description	Exchange of low denomination banknotes into higher denomination banknotes
Risk occurrence scenario (i.e. possible risk occurrence example)	Exchange of EUR low denomination banknotes into the EUR 200 banknotes to reduce the volume of carried cash.
Level of vulnerability	2
Justification for the level of vulnerability	Access to such services is very easy. Hiding the identification data of a person making the transaction is easy, especially when the individual transactions are made for the relatively low amounts. In many cases, proper identification and verification of the identity of the Ukrainian refugees is hindered. It is possible to execute the transactions of international nature, if such transactions are made at least partially as cashless transactions. All these service providers are the OIs. They are aware of their AML/CFT obligations. There is relatively few information on suspicious transactions/activity reported by the entities involved in foreign currency exchange[37]. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk.
Level of threat	2

[37] Excluding the banks providing the currency exchange service, including online.

Justification for the level of threat	Using the scheme of exchanging the low denomination banknotes into higher denomination banknotes for the purposes of terrorism financing is a widely available and inexpensive method. It can be perceived by the perpetrators as attractive. Physical carrying of banknotes intended for terrorism financing should not draw attention and reducing the volume of transported cash decreases the threat of its detection or accidental loss. Despite announcing of the decision on withdrawing the EUR 500 euro (since May 2019, the prohibition of printing these banknotes by the EURO-zone countries has been in force), no increased demand for these banknotes of the terrorist groups, which prefer the low-denomination banknotes, has been recorded in the EU Member States. However, the safety of this method requires planning and following the rule of executing low-value transactions. Exchange of crumpled, frequently dirty low-denomination banknotes may be easily noticed. In most cases, this method requires cooperation of the employees working in the institutions providing such services, such as a bank or currency exchange office. The GIFI has received very few information on using this method for terrorism financing purposes. CONCLUSION: Using the scheme of exchanging the low denomination banknotes into higher denomination banknotes poses a medium threat of terrorism financing.

Table 31

Type of used services, financial products	Non-cash currency exchange service providers
General risk description	Non-cash currency exchange combined with transfer of funds
Risk occurrence scenario (i.e. possible risk occurrence example)	Using non-cash currency exchange by the individuals associated with terrorist organisations in so called online currency exchange platforms to impede tracking of the transfer of assets path to the law enforcement authorities. For example – the funds in PLN are transferred to a so called online currency exchange platform from the bank account kept in one institution with the order of exchange into USD and transferring onto the account kept in the other bank, however in reality held by a different entity than the ordering party.
Level of vulnerability	2
Justification for the level of vulnerability	Access to the currency exchange services is very easy. Hiding the identification data of the person making the transaction is easy, especially when the individual transactions are executed in relatively low amounts. It is possible to execute the transactions of international nature, if such transactions are made at least partially as cashless transactions. There are also problems with verification of the foreign customers in the central registers of beneficial owners of the EU states, which refers in particular to the entities of complicated capital structure. All these service providers are the OIs. They have certain knowledge on their AML/CFT obligations. There is relatively few information on suspicious transactions/activity reported by the entities involved in foreign currency exchange. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level.

	The existing legislation partially corresponds to the scope of the analysed risk[38].
Level of threat	2
Justification for the level of threat	Using the scheme of non-cash currency exchange in so called online currency exchange platforms combined with transfer of funds to impede tracking the transfer of assets path to the law enforcement authorities is the identified method enabling terrorism financing. At present, the online currency exchange platforms are not regulated by law. They are neither subject to any act nor any authority, which would establish their scope of operation. The online currency exchange activity is not subject to the PFSA supervision. The PFSA supervision applies only to providing the payment services with respect to such activity, which requires obtaining the relevant authorisations. According to the estimates presented in the Accenture report [39] the estimated volume of trading on the currency market (excluding the inter-bank transactions and forward transactions) in 2019 in Poland reached nearly PLN 1 trillion. Within the next three years, the projected increase was of approx. PLN 86 billion. A noticeable drop in growth dynamics results from the economic crisis triggered by the outbreak of COVID-19 pandemic. Non-cash currency exchange combined with transfer of funds is relatively inexpensive and as a *modus operandi* may be perceived by the perpetrators as an attractive and widely available method of terrorism financing. In the conditions of dynamic growth of economic trade in the export or import enterprises, non-cash currency exchange transactions in the online currency exchange platforms can be relatively invisible for the supervision (in particular in the absence of clear legal regulations). The GIFI has received very few information on the opportunities to use this method for terrorism financing purposes. CONCLUSION: Using the scheme of non-cash currency exchange in so called online currency exchange platforms combined with transfer of funds poses a medium threat of terrorism financing.

The currency exchange services have been offered in Poland primarily by the stationary currency exchange offices conducting a regulated activity in the meaning of the *Act of 6 March 2018 – Business Operators' Law,* entered into the register of currency exchange business kept by the President of the National Bank of Poland. The currency exchange business is a regulated business activity consisting in purchase and sales of currencies and intermediation in their purchase and sales. However, due to the development of online technologies, the currency exchange service has been shared between the stationary currency exchange offices and online currency exchange platforms, which have started to gain popularity thanks to innovative solutions, offering non-cash and immediate currency exchange to their customers. The similar attitude was adopted by the banks, which have developed their own user-friendly currency exchange platforms. From the legal perspective however, the activity consisting in providing the remote currency exchange services with the use of the Internet to conclude the agreements and of the bank transfers to receive funds from the customers and send them to the customers, constitutes no currency exchange business in the meaning of the *Act of 27 July 2002 – Foreign Exchange Law.*

[38] Works on draft act amending the *Act – Foreign Exchange Law* and certain other acts, in the scope of covering the entities involved in non-cash currency exchange with the supervision. Pursuant to its assumptions, the "non-cash currency exchange transactions made by the online currency exchange platforms and the transactions of cash – non-cash currency exchange" are to be governed by the *Act of 18 August 2011 on payment services*. However, a part of service providers offering non-cash currency exchange and payment services at the same time has been already subject to the PFSA supervision.

[39] Report: RYNEK WYMIANY WALUT W POLSCE, https://www.accenture.com › _acnmedia › PDF-125

The fintechs, with their modern approach to currency exchange have recently gained on popularity by offering convenient applications and solutions to their customers. Apart from currency exchange and additional services, the fintech offer has been supplemented by the multi-currency pre-paid cards. According to the available data, the estimated annual turnover on the currency exchange market for 2020 amounted to nearly a trillion[40], while the value of this turnover continues to grow.

Vulnerability of the sector

All currency exchange service providers available in Poland – the stationary currency exchange offices, online currency exchange platforms and the banks are the obligated institutions (IOs). These entities have the statutory obligation to apply customer due diligence measures. Customer due diligence measures set out in the Act cover primarily the activities related to identification of the customer and verification of its identity; identification of beneficial owner; obtaining information on the purpose of customer relationships with the obligated institution; on-going monitoring of business relationships with the customer. The cases of occasional transactions of the value of EUR 15,000 or above are of particular importance for the currency exchange business, regardless of whether it is a single transaction or several transactions, which seem to be interlinked, or a transfer of funds of the value above EUR 1,000. Another issue of importance from the perspective of customer due diligence is the doubts as regards the correctness or completeness of already obtained identification data of a customer as well as the case of suspected money laundering or terrorism financing.

The currency exchange business (regulated activity performed under the *Act of 6 March 2018 – Business Operators' Law*) can be conducted by a natural person, who has not been convicted for a tax offence, or an offence committed for the purpose of financial or personal gain, a legal person, or organisational unit without legal personality, in which the partners entrusted with management of the company's affairs, or authorised to represent the company, or the members of the management authorities have not been convinced for the abovementioned offences. The requirement of clean criminal record applies also to the persons managing the activities related to conducting a currency exchange business and to the beneficial owner of an entity involved in the currency exchange business and the persons directly performing the activities of the currency exchange office. In addition, the persons directly performing the activities of the currency exchange office must have documented the professional preparation to perform these activities i.e. a completed a course covering the currency exchange business-related issues or working in the bank for at least 1 year as a person handling the currency exchange transactions. There are also relevant restrictions in performing the currency exchange business, related to the necessary equipment of the premises intended for the currency exchange business and the method of keeping the records and issuing the bills of purchase and sales of foreign currencies. These are set out in the Regulation of the Minister of Finance of 24 September 2004. In addition, each currency exchange office operator is obliged, for the purposes of tax control and control performed by the President of the National Bank of Poland (regulated activity), to keep the documents related to this activity for the period of 5 years, starting from the end of a calendar year, in which the operator performed the currency exchange business. These requirements do not apply to the online currency exchange platforms, operation of which is not the activity based on the entry into the register kept by the President of the National Bank of Poland.

[40] https://www.accenture.com › acnmedia › PDF-125 RYNEK WYMIANY WALUT W POLSCE – Accenture access on 14.01.2023

The currency exchange sector entities have certain awareness of their AML/CFT obligations[41]. There are relatively few suspicious transaction reports submitted to the General Inspector of Financial Information (GIFI) originating from the entities involved in the currency exchange. According to the GIFI data on the analytical proceedings initiated by the GIFI in 2019-2021, in 2019 these accounted for approx. 0.5% of all proceedings on the suspected money laundering or terrorism financing linked to the use of currency exchange or banknote exchange for suspicious transactions, in 2020 these accounted for approx. 0.9% and in 2021 for approx. 0.8%.

The employees of the stationary currency exchange offices should have a relatively high awareness of the exposure of the office operation to suspicious transactions related to money laundering or terrorism financing. They are obliged to complete the relevant course for the currency exchange office employees, which cover the practical and legal aspects of running such activity. The course must be documented with the acquired certificate or statement. Thus, such employees should be trained in analysing the warning signals during the suspected transactions. Since vast majority of the currency exchange offices in Poland belongs to the small and medium-sized enterprises sector, only a few of them have deployed the advanced IT tools and systems supporting the delivery of the anti-money laundering and counter-terrorism financing objectives. Since 2019, the National Bank of Poland has been organising the meetings with the currency exchange business operators aimed at propagation of knowledge on the activities of the currency exchange offices and anti-money laundering and counter-terrorism financing. the GIFI has carried out trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of customers as well as reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) were provided. In addition, the trainings raising the AML/CFT awareness in the obligated institutions have been carried out.

A relatively large number of currency exchange transactions executed in Poland are occasional transactions i.e. not resulting from business relationships. The individual customers declare that 44% of their funds[42] were exchanged in the stationary currency exchange offices. Popularity of such currency exchange is primarily affected by the anonymity of the occasional transactions, frequently executed below the threshold of equivalency of EUR 15,000 and cash-based nature of the offered services.

Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of individuals. The existing language and cultural barrier significantly affects proper identification of the increased risk factors. This barrier makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. Considering however the increasing economic activity, one should also realise that the currency exchange in small and medium-sized enterprises is a natural and common phenomenon. 54% of them performs it at least several times a week, and as many as three among four enterprises of such type performs the currency exchange operations once a week or more rarely. From the perspective of a currency exchange office, there are problems with verification of e.g. foreign customers in the central registers of beneficial owners of the EU state, which applies in particular to the entities of complicated capital structure.

[41] In 2021, the controls covering 842 currency exchange offices were performed. Irregularities in the area of anti-money laundering and counter-terrorism financing were identified in 100 from among the controlled currency exchange offices.

[42] https://www.accenture.com › acnmedia › PDF-125 RYNEK WYMIANY WALUT W POLSCE – Accenture, access on 14.01.2023

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

In terms of assessment of money laundering and terrorism financing threat, the currency exchange sector is one of the most commonly used sectors. The money laundering or terrorism financing perpetrators must in some cases convert the available funds between various currencies. The funds may come from legal or illegal sources. This modus operandi is of particular importance for terrorism financing, when the funds are collected for the purposes of travel to the conflict zone by the fighters, so called foreign fighters, for the purposes of transmitting the funds to specific terrorist organisations or for specific ideological goals related to the conflict in the other region of a continent or the globe.

From among the identified threats in the currency exchange area, the focus should be primarily on the possibility of infiltration of the currency exchange offices by the criminal groups. This applies in particular to the currency exchange offices located in the border zones, in the cities being a popular destination for tourists using various currencies. The factor increasing the threat of using a currency exchange office for money laundering is provision of services to the politically exposed persons (PEPs). The money laundering and terrorism financing threat is also increased by using cash in the transaction. This can be of particular importance in relatively low-amount currency exchange transactions. Apart from currency exchange in cash, the key identified threats include: anonymity of transactions, vicinity of border areas, presence of migrant communities at the territory of the country (economic migrants, refugees, cross-border workers, individuals applying for asylum and tourists).

Another threat factors in the currency exchange area encompass the threats related to the currency exchange business operator. This applies to the opportunity of blending the profits from legal and illegal sources; relatively high volume of trading in the single currency without economic justification; failure to ensure due diligence by the currency exchange office employees when performing the duties related to the customer due diligence measures; establishing the relations without a physical presence of the customer; transferring funds on the currency accounts of third persons without the possibility to determine the beneficial owner of the transaction; possibility of using high denomination banknotes (e.g. EUR 500 and 200), used among others to transfer and keep the profits from illegal activity; product threat – purchase/sales of foreign exchange assets in the currency exchange office and transactions through the accounts or with the use of automatic currency exchange machines. Executing the transaction using the automatic currency exchange machine enables maintaining anonymity. In addition, one should put attention to the threats related to personal links between the currency exchange business operators and the high risk states by contacts with the entities established or having business ties in the countries of increased risk of money laundering or terrorism financing, listed in the *Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016* and on the FATF lists. The focus should be also on the currency exchange offices combining a short period of market activity with high turnover.

The threats are also related to the customers of the currency exchange offices. These include the threat related to dispersion of the transactions. In order to avoid the obligation of notifying the GIFI on transactions above EUR 15,000, the transactions of slightly lower value and distributed in time are executed. The threat increases in the case of a high number of foreign exchange offices located in direct vicinity from each other, for example at the same street. The threat accompanying the currency exchange related to customer service encompasses also the customers executing the anonymous bearer transactions, which are confirmed by the bill of purchase/sales containing no identification data of the

customer. The risk is affected primarily by the anonymity of the occasional transactions, especially if they are executed below the threshold of equivalence of EUR 15,000.

Currently, the distant identification and verification of the customers' identity, which becomes a standard, seems to be a threat. This is associated with impeded possibility to verify the authenticity of the presented documents and difficulties with assessing the customer's behaviour.

Averaged level of threat of the other currency exchange sector – ML – 3.33 and FT – 2.0

Averaged level of vulnerability of the other currency exchange sector – ML – 2.33 and FT – 2.0

Estimated level of probability for the sector – ML – 2.73 and FT – 2.00

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the currency exchange sector – 1.80	
1 – 1 .5	Low
1 .6 – 2 .5	Medium
2 .6 – 3 .5	High
3 .6 – 4	Very high
ML risk of the currency exchange sector– 2 .64	
1 – 1 .5	Low
1 .6 – 2 .5	Medium
2 .6 – 3 .5	High
3 .6 – 4	Very high

CONCLUSION 1: The level of risk of using the currency exchange sector for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the currency exchange sector for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the currency exchange sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The currency exchange sector should undertake the actions guaranteeing maintenance of high awareness of exposure to the crime of money laundering and terrorism financing, as well as maintaining the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

The currency exchange sector entities should enhance their activities related to appropriate assessment of the executed currency exchange transactions as well as to maintain on-going monitoring of business relationships.

The currency exchange sector should undertake the actions enhancing the awareness of exposure to the crime of money laundering and terrorism financing, as well as increasing the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

Since only a few currency exchange offices have deployed the advanced IT tools and systems supporting the implementation of the anti-money laundering and counter-terrorism financing objectives, it is reasonable to develop their capacity in this area by the currency exchange sector institutions.

The trainings for the obligated institutions from the currency exchange sector, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be continued. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The obligated institutions from the currency exchange sector should put particular attention to the currency exchange transactions linked to the jurisdictions of higher risk of money laundering and terrorism financing. The obligated institutions should place particular emphasis to determination of data on the source of origin of transferred assets as well as documents justifying the specific transaction. In the event of exchange of higher volume of cash by the non-EU residents, the obligated institutions should consider requesting the customer to provide information on the source of origin of the assets, for example by verification of the declarations of foreign currency of the customers from the states outside the EU.

The obligated institutions accepting the payments or cash deposits in foreign currencies should verify the source of origin of the assets, taking into account that obtaining information confirming the currency exchange or confirming the submission of declarations of foreign currency from the customer could be reasonable.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance. The currency exchange sector should put particular attention to the high-volume

transactions made with the residents of the jurisdictions in the conflict zones as well as to the transactions indicating that they were executed with the use of an intermediary for the currency exchange purposes.

6. Area – virtual currencies

Sector description - is contained in sub-chapter 2.1.2. of NRA "Financial market sectors", subchapter 4.5. "Register of trust and company service providers and the register of virtual currency service providers" and in subchapter 7.2.1 – "Vulnerability of the financial market" as well as in chapter 5.3 "The most common methods used to finance terrorism".

Risk occurrence scenarios (i.e. possible risk occurrence examples) both for money laundering and terrorism financing – referred to the use of financial products and services in the form of decentralized and convertible virtual currencies (so called cryptocurrencies). Their description is presented below.

Money laundering

Table 32

Type of used services, financial products	Decentralized and convertible virtual currencies (so called cryptocurrencies)
General risk description	Use of cryptocurrencies to transfer the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Use of cryptocurrencies to gain profits from various offences, including extortions (for example as a payment for deciphering of hacked computer data), abductions (as a ransom for freeing a kidnapped person). 2. Use of cryptocurrencies to pay for drugs bought via the commercial platforms in Darknet. 3. Use of cryptocurrencies to obfuscate the source of origin of illegal profits, for example money transferred in effect of unauthorised access to the bank account of the victim are deposited on the bank account of the virtual currency exchange platform operator to purchase the cryptocurrency units. The purchased cryptocurrency units are then transferred onto the anonymous *offline* wallet. 4. Depositing on the account in a Polish bank of the funds, which may be the proceeds of crime, followed by their transferring to the entities involved in cryptocurrency trading (impeded/impossible tracking of further part of the funds flow). 5. Providing the financial intermediation services among others in the area of investments in cryptocurrencies by the entities holding no applicable authorisations. 6. Use of so called BTMs (Bitcoin ATMs) for the purposes of cash withdrawals in various currencies. Cash transactions enable legitimisation of the proceeds of crime. 7. Using so called decentralized finance - DeFi[43] by the offenders. DeFi is a catch-all term referring to the financial services that exist on public blockchains (mostly *Ethereum*). DeFi can be used to execute the same transactions which are handled by the banks, for example incur and grant loans, purchase the insurances, trade in derivatives, trade in assets without involvement of any third parties.
Level of vulnerability	3
Justification for the level of vulnerability	Access to this type of services is relatively easy. It is possible to hide identification data of customers (the service providers identify the customers distantly). Transactions of international nature are possible. The virtual currency (including cryptocurrency) exchange service providers, or the providers of so called "hot wallets", are the OIs. Although the Internet provides access to the offers of entities registered outside the country and the EU, which are not subject to the AML/CFT obligations, the transactions with the

[43]DeFi is of global, *peer-to-peer* nature (i.e. directly between the two persons rather than by the centralised system), provides anonymity and global accessibility.

	use of cryptocurrencies can be made without the intermediation of any third entities. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on this type of services, however originating from the entities being the OIs or made available by a foreign financial intelligence unit. It is probable that the case of money laundering in the scope of the analysed scenarios will not be detected The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation partially corresponds to the scope of the analysed risk.
Level of threat	3
Justification for the level of threat	Use of cryptocurrencies for transferring the assets from illegal sources can be one of the money laundering methods. The reason behind this is that the natural features of cryptocurrencies enable relatively easy hiding of data of the transaction parties, making it difficult to track the transfers' path[44] and their potential stopping. This encourages their use by the organised crime groups, especially that such transactions are difficult to identify by the law enforcement and tax authorities. Applying this *modus operandi* for money laundering requires however relevant planning as well as appropriate knowledge. The GIFI has few information on the options of using cryptocurrencies to transfer the assets from illegal sources. CONCLUSION: At the current stage, using the cryptocurrencies to transfer the assets from illegal sources poses a high risk of money laundering due to the level of complexity.

Table 33

Type of used services, financial products	Centralized virtual currencies
General risk description	Use of centralized virtual currencies to transfer the assets from illegal sources
Risk occurrence scenario (i.e. possible risk occurrence example)	The offenders exchange illegal money into the centralized virtual currency units in one of the online cryptocurrency trading points executing such transactions. Then these currency units are deposited on the account opened at a foreign service provider offering the funds transfer services (similar to payment services). These currency units are transferred onto the other accounts opened within the same transaction system and then, following their conversion, transmitted onto a foreign bank account.
Level of vulnerability	3
Justification for the level of vulnerability	Access to this type of services is relatively easy – although there are few entities offering such currencies. It is possible to hide the identification data of customers (these service providers identify the customers distantly). Transactions of international nature are possible. These service providers are the OIs, however the Internet provides access to the offer of entities registered outside the country and the EU, which are not subject to the AML/CFT obligations. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) has limited capabilities to collect and analyse information on this type of services. It is

[44] In particular in the case of using the transaction mixing and muddling tools to complicate the links between the transactions and their users (so called *anomizers*).

	probable that the case of money laundering in the scope of the analysed scenarios will not be detected The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation partially corresponds to the scope of the analysed risk.
Level of threat	3
Justification for the level of threat	Use of centralized virtual currencies to transfer the assets from illegal sources can be one of the money laundering methods. The global nature of the financial and capital markets enables relatively easy conversion of the illicit proceeds into the centralized virtual currency units and (in effect of a transaction chain) and aback (using the anonymisation of the transaction parties and features impeding transfer tracking and stopping). Applying this *modus operandi* requires however relevant planning and the applicable knowledge. The GIFI has information on the possibilities to use the centralized virtual currencies to transfer the assets from illegal sources. CONCLUSION: At the current stage, using the centralized virtual currencies to transfer the assets from illegal sources poses a high threat of money laundering.

Terrorism financing

Table 34

Type of used services, financial products	Decentralized and convertible virtual currencies (so called cryptocurrencies)
General risk description	Use of cryptocurrencies to transfer the assets for the purposes of terrorist activity
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Propagation of information on the cryptocurrency addresses, at which the supporters of terrorist organisations transfer the assets in the decentralised and convertible virtual currencies. 2. Collecting funds from the supporters of terrorist organisations or unaware investors under the pretext of financing the preparations to the issuance of a new cryptocurrency, which is either not performed, nor ends with depreciation of the issued currency. The collected funds are provided to a terrorist organisation. In addition, a system of orders aimed at effective recruitment of the new organisation members may be implemented. 3. Donations of virtual currencies made by the relatives of the terrorist organisation fighters via the OTT (Over the Top) application. The over-the-top (OTT) application is any application or service, which provides the product via Internet and bypasses the conventional distribution.
Level of vulnerability	3

Justification for the level of vulnerability	Access to this type of services is relatively easy. It is possible to hide identification data of customers (the service providers identify the customers distantly). Transactions of international nature are possible. The virtual currency (including cryptocurrency) exchange service providers, or the providers of so called "hot wallets", are the OIs. Although the Internet provides access to the offers of entities registered outside the country and the EU, which are not subject to the AML/CFT obligations, the transactions with the use of cryptocurrencies can be made without the intermediation of any third entities. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on this type of services, however originating from the entities being the OIs or made available by a foreign financial intelligence unit. It is probable that the case of money laundering in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation partially corresponds to the scope of the analysed risk.
Level of threat	3
Justification for the level of threat	Using virtual currencies to transfer the assets for the purposes of terrorist activity can be one of the methods of providing financial support to terrorism due to their features promoting anonymisation of the transaction parties and impeding both transfers' tracking and stopping. The virtual currencies themselves have gained on popularity due to their features, such as global availability, easy access, reliable and irreversible transactions, low cost and swiftness of international transfer. It seems however that their use in Europe by the terrorist organisation is relatively low compared to the development of their popularity in the Supranational organised crime groups, especially these linked to cybercrime. The TE-SAT Europol report for 2020 concludes that the number of cases related to the use of cryptocurrencies for terrorism financing in 2020 remained at a low level. Use of cryptocurrencies is difficult to apply, requires specialist knowledge. CONCLUSION: Use of cryptocurrencies to transfer the assets for the purposes of terrorist activity poses a medium threat of terrorism financing.

The crypto-asset market is of supranational nature, breaking out of the territorial nature of a regulated activity. In Poland, the crypto-asset market is also neither the regulated, nor supervised market. The PFSA provides neither the licences, supervision, nor enforces any other supervisory powers as regards the cryptocurrencies trading activity[45]. Some entities operating on the cryptocurrency market are authorised to provide the payment services used in particular to settle the payments made with the legal tender (FIAT) for purchased or sold cryptocurrencies. In this scope, the activity of these entities is subject to the PFSA supervision. One should emphasize however that this supervision covers only the regularity of providing the payment services and includes no compliance of these entities or persons represented by them with the obligations under the purchase or sales of cryptocurrencies.

Since October 2021, conducting a business activity in the area of virtual currencies has had the status of a regulated activity i.e. depends on the earlier entry into the register of virtual currency activities, kept by the Head of the Revenue Administration Chamber in Katowice (815 entries as of 29 June 2023).

[45] https://www.knf.gov.pl/komunikacja/komunikaty?articleId=70400&p_id=18, Warning against the fraudsters referring to the PFSA supervision in the scope of cryptocurrency exchange transactions, access on 20.01.2023

Article 2(2)(26) *of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism* provides for a legal definition of virtual currencies. Pursuant to this provision, the "virtual currency" shall be understood as a digital representation of value that is neither:

a) a legal tender issued by the National Bank of Poland, foreign central banks o any other public administration authorities,
b) an international unit of account established by an international organisation and accepted by the individual member or cooperating countries,
c) electronic money in the meaning of the Act of 19 August 2011 on payment services,
d) a financial instrument in the meaning of the Act of 29 July 2005 on trading in financial instruments,
e) bill of exchange or cheque,

and is exchangeable in trading into legal tenders and accepted as a mean of exchange as well as can be transferred, stored or traded electronically.

Due to rapidly evolving technologies and products of the cryptocurrency market, the European Union decided to cover the crypto-assets, crypto-asset issuers and crypto-asset service providers (trading platforms for crypto-assets and crypto-asset wallets). This aims at ensuring greater transparency in the European Union, since only some member states have implemented the national regulations on crypto-assets, while there has been no specific regulatory framework at the EU level. To this end, the *Regulation of the European Parliament and of the Council (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937* (MiCA - Markets in CryptoAssets) was issued. The draft Regulation contains the requirements for the entities willing to involve in the crypto-asset trading. For example, it introduces the obligation of obtaining the authorisation o publishing a relevant information document, which will be approved by the competent national authorities. In addition, the organisational and prudential safeguards requirements will be amended. The *Regulation on markets in crypto-assets* divides the crypto-assets into 3 categories – asset-reference tokens; e-money tokens; crypto-assets other than tokens. In the asset-reference tokens and e-money tokens categories will require obligatory acquisition of a formal authorisation, obtaining of which will depend on meeting many conditions. These conditions include having the appropriate procedures and policies implemented or having the relevant staff of adequate knowledge and experience. The requirements for the members of the management body, in particular in the scope of the impeccable character, were also established. In general, the companies providing the cryptocurrency services must be highly transparent to the authorities controlling their operation at the territory of Poland. The regulation provides for also the new category of entities "providing advice on cryptocurrencies". This includes various types of advisors inducing to make investments in digital assets. Only the legal persons having their registered office in the Member State of the European Union may apply for authorisation. The authorisation is available to the cryptocurrency issuers, who offer the asset-referenced tokens to the public in the Union or seek the admission of such tokens to trading on the trading platform for crypto-assets. The authorisation granted by the competent authority is valid for the entire Union and shall allow an issuer of an asset-referenced token to offer to the public, throughout the Union, the asset-referenced token for which it has been authorised, or to seek an admission to trading of such asset-referenced token on the trading platform for crypto-assets. The provisions of the Regulation shall apply by 30 December 2024, excluding the provisions on the asset-referenced tokens and e-money tokens, which shall be valid by 30 June 2024.

Another legal act in the area of crypto-assets is the *Regulation of the European Parliament and of the Council (EU) 2023/1113 of 31 May 2023 on information accompanying transfers of funds*

and certain crypto-assets and amending Directive (EU) 2015/849. This Regulation forms a part of the package of amendments to the EU regulations concerning the anti-money laundering and counter-terrorism financing[46]. The amendment of the regulations involves covering the transfers of crypto-assets with similar requirements for information, which must be provided with the transfers of crypto-assets, to the requirements applied for transfers of funds. The crypto-asset service providers will be obliged to collect and make available information identifying the sender and recipient of the transfers of crypto-assets. This information will have to be provided with the transfer of crypto-assets. The amended regulations will enable tracking the transfers of crypto-assets. The Regulation shall be valid by 30 December 2024.

In parallel to the works on the regulation on the markets in crypto-assets, the European Commission, on 8 December 2022, published the proposal for a Directive on administrative cooperation covering the tax reporting on cryptocurrencies ("DAC8"). The Commission proposed […] harmonisation of the reporting regulations for the service providers harmonising the transactions in digital currencies, including annual stock exchange and cryptocurrency market reports[47]. This will enhance transparency in the area of tax liabilities, supporting identification of taxable income and profits. As a matter of principle, the crypto-asset service providers, regardless of their size or location, will be obliged to report the transactions of customers resided in the EU, regardless of whether these are national or cross-border transactions. The new directive will improve the capacity of the Member States to detect and counteract tax frauds, tax evasion and tax avoidance. It will also extend the scope of reporting and information exchange between the tax authorities in the EU by covering income and revenue generated by the users resided in the EU, who conduct the activity with the use of cryptocurrencies. The directive concerned may set the end of the period, when the owners of cryptographic wallets could remain anonymous. The issue of determination of the personal data of the asset owners is the key for effective verification of natural and legal persons, who may evade from taxation. The directive provides also for comprehensive reporting obligations. The reportable transactions include the exchange transactions and transferred related to crypto-assets. The scope of directive covers both the national and cross-border transactions.

In the sector of business operators providing the virtual currency services, the increasing threat related to money laundering and terrorism financing has been posed by non-fungible tokens (NFT). These are the unique digital certificates based on the blockchain technology, which represent a differently defined right to both physical and digital assets. By way of affordable and credible record of rights and opportunity to earn royalties from the initial sales of a digital asset – the NFT market has become one of the most rapidly developing sectors of the global digital economy. The NFT sector is the sector requires no precise information on the customers and transactions. No AML regulation on the NFT market leads to a higher risk to the market participants, and in more general terms for the overall financial stability. NFTs are based on the same blockchain technology as the virtual currencies, provided

[46]This package consist in, apart from the legal act discussed in this material, the following proposals: Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421), Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420), Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorism financing and repealing Directive (EU) 2015/849 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423).

[47]https://kryptoprawo.pl/dac8-transakcje-kryptowalutowe-beda-raportowane-do-skarbowki/, access on 22.01.2023

that they are non-fungible. NFTs are the cryptographic tokens developed under the blockchain-based technologies and associated with a specific digital object. This digital association represents the inherent right to a digital or physical asset, including images, films, audio files or other digital "items". The NFT functions are managed using the smart contracts and digital wallets, while in general these activities are publicly verifiable, since they are registered in blockchain.

At present, there are in general no regulations pertaining to the NFT transactions. FATF notes however that the NFT transactions may be addressed by the definition of virtual assets, provided that they are for payment or investment services in practice. In the Polish conditions, an entity offering NFTs and meeting the virtual currency criteria in the meaning of the *Act on counteracting money laundering and financing of terrorism*, will be the obligated institution. The obligated institutions with established business relationships with such entity (for example the banks keeping the bank account for such entity), should consider this fact in assessment of business relationships with the entity. They should in particular consider the fact that the purchase and sales of NFTs are made with the use of virtual currencies. In the Polish legal system however, making the virtual currency exchange transactions to NFTs that guarantee anonymity is prohibited.

Vulnerability of the sector

The virtual currency (including cryptocurrencies) exchange service providers or providers of so called "hot wallets" are the obligated institutions. The Internet however provides access to the offer of entities registered outside Poland and the EU, which are not covered by the AML/CFT obligations. The fact that the cryptocurrency transactions can be made without the intermediation of any third parties also needs to be noticed. These entities, as the obligated institutions, apply the customer due diligence measures laid down in the Act of 1 March 2018 on counteracting money laundering and financing of terrorism.

The customer due diligence measures listed in the Act cover in particular proper identification of the customer and beneficial owner, monitoring of discrepancies between the Central Register of Beneficial Owners (CRBO) and the findings of the obligated institution, proper determination of the ownership structure and control in the case of a customer being a legal person or an organisational unit without legal personality. This includes also the on-going monitoring of business relationships of the customer, obtaining information on their purpose and intended nature. Application of customer due diligence refers to the occasional transactions equal to EUR 1000 or above.

However, according to the obtained information, the operation of the entities (obligated institutions, in particular smaller ones, covering the cryptocurrency trading points, cryptocurrency exchanges, cryptocurrency wallet providers) offering the services in the area of virtual currency exchange, entails the difficulties in actual monitoring of transactions of their customers. The virtual currency sector entities are aware of their AML/CFT obligations to a diversified extent.

In the scope of the virtual currency sector, in 2019-2021 the GIFI received and examined 45 analytical cases in total, where the suspicious transactions were the transactions made with the virtual currencies. In 2019, they accounted for approx. 1.8% of all investigations concerning money laundering or terrorism financing with regard to the use of virtual currencies for suspicious transactions, in 2020 of approx. 2.0%, while in 2021 of approx. 4.6%.

With regard to the transactions in the virtual currency sector, the fraudulent entities use the attribute of public authority reliability. This covers the offers of purchase of sales of cryptocurrencies, with simultaneous emphasis that these transactions are supervised by the Polish Financial Supervision Authority. The potential customers are frequently informed that the transactions will meet the "PFSA

requirements on recording the transaction process", which is supposed to consist among others, in providing access to the computer desktop. These entities frequently communicate that the virtual currency exchange operation will be made with participation of the Office of the PFSA officer to monitor the course of transaction.

The Central Cybercrime Bureau notices that distinguishing trend of the crime in cyberspace and in the offences committed with the use of the state-of-the-art technologies consisting in the use of cryptocurrencies to hide the sources of the proceeds of crime. This includes the virtual currencies covering cryptocurrencies and certain other conventional units that are convertable to fiduciary money, which can be used to transfer the assets also for the purposes of terrorist activity. This is facilitated by the anonymisation of the parties to the transactions, which hinders both tracking the transfers and their stopping.

According to the Prosecutor's Office practice of criminal cases, the cases related to virtual currencies are highly complicated[48]. This results among others from the fact that controlling the virtual currency exchange service providers and the transactions themselves is less effective compared to the "conventional" flow of non-cash money. The experience demonstrates that the operation of vast majority of VASPs (Virtual Asset Service Providers) more or less touches the shadow economy of the criminals' activity, while still unrecognized nature of the digital tokens increases the risk of fraudulent conversion of funds. This is facilitated by the absence of a consistent global supervision over the service providers, different legal regulations or even the places with no effective AML/CFT procedures and implementation of the KYC standards. Another point is that the alternative costs resulting from loss of reputation are relatively low: revealing by the bank of the "laundering"-related event will most probably trigger the negative social relations, even if the AML rules have actually worked. In the case of cryptocurrency exchanges and trading points, the money laundering opportunity frequently triggers the opposite response: the offenders willingly make use of the "suspicious" platforms, which increases profits of their administrators.

According to the studies of P. Opitek[49] conducted on the basis of the investigations of all Prosecutor's Offices in Poland in the last several years (until 2020) on the cryptocurrency crime, the unit which is most frequently used to commit crimes is bitcoin, and against the common opinion, the systems providing even greater anonymity (Z-Cash, Monero) are used much less frequently. This results primarily from the fact that the BTC market is relatively deep, scalable and stable.

According to the report of the Chainalysis company involved in blockchain analysis, the value of illegal transactions on the cryptocurrency market in 2022[50] amounted to USD 20.1 billion. This stems primarily from their use by the companies covered by the US sanctions. The temporary breakdown of the cryptocurrency market in 2022 was the effect of a collapse of stock exchanges and reducing the risk acceptance level. The investors have suffered major losses, while the regulatory companies have intensified their calls for increasing the consumer protection. However, according to the Chainalysis report, even when the general volume of transaction dropped down, the value of transactions with cryptocurrencies linked with the illegal business activity or even criminal activity has increased for the second subsequent year. The reason behind this was the transactions linked to the sanctioned entities. In 2022 they accounted for 44% of illegal activity on the cryptocurrency market. The example can be the Russian cryptocurrency exchange – Garantex – sanctioned by the U.S. Department of Treasury in April 2022. According to the report, its operations covered "a significant part of the illegal transaction volume

[48] P. Opitek – Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych, Prokuratura i Prawo 12, 2020
[49] Ibidem
[50] https://isbiznes.pl/2023/01/13/przestepcy-lubia-kryptowaluty/, access on 19.01.2023

in 2022", provided that the vast majority was generated by the "Russian users operating on the Moscow stock exchange". Most probably, the cryptocurrencies were the measure to transfer money out of Russia. Since the company is sanctioned, all these transactions were labelled illegal. In 2022 the volume of transactions with cryptocurrencies linked to frauds, ransomware, terrorism financing and human trafficking decreased, while the volume of transactions in stolen cryptocurrencies increased by 7%.

As for Poland, the Chainalysis report defined (data from September 2021 to September 2022) the total value of funds received in this time by Poland for USD 63.62 billion, which accounts for -0.22% of increase compared to the previous year. Chainalysis identified the value of USD 384.0 million of illegal trading and USD 749.0 million of suspicious activity in this period.

The largest category of activity in Poland was the centralised exchange, with the inflow from the entire activity of 74.9% in the period between September 2021 and September 2022. The second largest category in Poland was DeFi with 22.3%.

The most frequently used platform in Poland in terms of network traffic is the Binance.com exchange, which was visited 30.7 million of times between September 2021 and September 2022. The second largest platform was the hosted wallet named eToro.com, which recorded 12.25 million of visits in the same period.

The illegal activity in the field of virtual currency trading identified in Poland between September 2021 and September 2022 has changed. The greatest source of illegal activity stemmed from the sanction category. In this category, the cryptocurrency of the value of USD 74.47 million were received in the a/m period. The most dynamically developing category of crime were the stolen funds, value of which increased by 7.3% compared to the previous 12 months, reaching the total value of USD 26.58 million.

Due to the fact of growing popularity of the NFT technology, the virtual currency service providers are recommended to put particular attention to the suspicious wallets and NFT transactions. These institutions may provide their services in the field of virtual currency exchange into NFTs only when they do so with the use of transparent virtual currencies. The GIFi emphasizes that using so called AEC (Anonymity Enhanced Cryptocurrencies) for such exchange is prohibited. Using these anonymity enhanced cryptocurrencies results in the inability to prove that a given obligated institution fulfilled the obligation of applying the customer due diligence. One should note however that the NFT market has been evolving into the secondary market, which may require implementation of specific regulations preventing the increase of money laundering and terrorism financing risk on the discussed market.

The NFTs are particularly vulnerable to money laundering and terrorism financing due to their similarity to the works of art and the applied blockchain technology.

NFT vulnerability in this field is associated with the specific nature of trading in the works of art in the more extensive NFT domain. On the poorly regulated NFT market, this specific nature is characterised by: high level of anonymity, limited information on the purchasers, self-regulating markets, non-transparent prices and high value transactions between the unknown parties. The NFT market is vulnerable to fraudulent practices and the activities of the law enforcement authorities in the case of frauds involving the NFTs are significantly impeded.

Another cause of vulnerability is the easiness to transfer the right to NFTs, inherently associated with the basic blockchain technology. Similarly as in the case of virtual currencies, transfer of right to the NFTs is not limited by the geographic boundaries and is made without the potential regulatory intervention of incurring any costs. The right to NFTs may be therefore quickly transferred from one entitled person to another and between different wallets and ultimate beneficiaries. This makes the

recording of assets by the tax or other authorities very difficult, since the jurisdictional status of NFTs is unclear.

The next vulnerability consists in hiding of basic data concerning the virtual currency transaction. Although the change of NFT ownership between the wallets can be tracked, the change of the wallet address does not reflect the change of the owner. Since vast majority of the main NFT platforms requires no customer identification and applies no customer due diligence measures towards the customer, the ultimate owner wallets must be mapped using the transaction bocks, to see the chain of the wallets via which the currency has passed. This process becomes more complicated due to the virtual currency "mixers" or "tumblers".

The increased vulnerability of NFTs is associated with the easiness to hide the wallet ownership. As the wallet beneficiaries are located, these need to be assigned to a legal or natural person. The virtual currency wallets are pseudo-anonymous in many jurisdictions, and identification of the responsible person may require identification of the relevant IP address, used hardware and other factors that may involve various jurisdictions.

According to information held by the GIFI, the virtual currency sector institutions should analyse data on the transactions and have the deployed tools to assess the event logs. Due to the costs of maintaining the advanced dedicated IT tools, not all institutions in this sector have deployed such advanced automatic tools and IT systems, which support the achievement of the anti-money laundering and counter-terrorism financing objectives.

In order to raise the AML/CFT awareness in the obligated institutions – including in the virtual currency sector, the GIFI has carried out trainings for the obligated institutions and cooperating units, during which the theoretical and practical guidelines on anti-money laundering and counter-terrorism financing issues were provided. This included among others determining the beneficial owner and the ownership and control structure of customers as well as reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO). The level of AML/CFT awareness in the obligated institutions of the virtual currency sector concerned has improved significantly.

Due to the pending military conflict in Ukraine, obtaining a wider spectrum of documents confirming the identity or reliability of a customer is impeded. The problems with the identification and verification of the persons are present also in this sector and the existing language and cultural barrier significantly affects proper recognition of the increased risk factors. There are also difficulties with verification of the foreign customers in the central registers of beneficial owners of the EU states, including in particular the entities of a complicated capital structure.

Access to the services offered by the virtual currency sector providers is relatively easy. It is possible to hide the identification data of customers (such service providers may identify the customers remotely). There are transactions of complicated and cross-border nature.

The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on this type of services, however originating from the entities being the OIs or made available by a foreign financial intelligence unit. It is probable that the case of ML or FT in the scope of the analysed scenarios will not be detected.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation partially corresponds to the scope of the analysed risk.

Threats in the sector

The volume of trading in the cryptocurrency market has been increasing practically every year, both in terms of processed transactions and the number of customers of the companies operating on this market. The absence of sufficient transparency of transactions and difficulties with identification of the ultimate customers involved in transactions on this market seem to be most important threat factor in this market. This may facilitate money laundering or terrorism financing.

Although the currency most frequently used for criminal purposes in the Polish conditions is bitcoin, Europe shows certain trends of change towards the anonymity enhanced cryptocurrencies, which ensure greater anonymity of transactions. The anonymity enhanced cryptocurrencies are however more difficult to acquire on the market and to make transactions compared to bitcoin.

In the virtual currency sector, the identified area of activity of particular risk of money laundering and terrorism financing is the area of operation of cryptocurrency exchanges/trading points acting as the intermediaries of exchange of virtual assets handled by the financial institutions and their use for transferring the proceeds of crime. The GIFI identified a significant growth in the number of natural persons acting as so called partners of the other obligated institutions involved in the cryptocurrency exchange, leading to difficulties with examining the source of origin of the funds. In addition, there are cases, in which the entities operating as the cryptocurrency exchanges/trading points had no relevant tools/software to ensure on-going monitoring of the customer transactions and identification of suspicious transactions. From this reason, the sources of origin of cash were not examined, no analyses of the cryptocurrency addresses with a view to the source of origin and legality of the transacted cryptocurrency units were performed and no analyses of transactions non-compliant with knowledge about the customer and generating very high risk of money laundering and terrorism financing both on the cryptocurrency exchange/trading point and at the level of a financial institution keeping the accounts of these entities were performed. With regard to the above, since the transactions made by the agency of such entities are difficult to track due to the specific nature of the applied technology, the obligated institutions should thoroughly examine the source of origin of funds of the supported cryptocurrency exchanges/trading points.

The opportunity of quick transactions between different jurisdictions, in which the information obligations related to transfers of virtual assets have not been fully implemented yet, may pose a threat. In these jurisdictions, the obligation to reveal the identity of the entity making a transaction with virtual currencies may also not be implemented.

In terms of assessment of money laundering and terrorism financing threat, the virtual currency sector is potentially the sector used with regard to predicate offences for money laundering and terrorism financing: tax offences, drug trafficking, property and trading offences, corruption, human trafficking or frauds.

Since the exchange of virtual assets becomes increasingly regulated in the anti-money laundering and counter-terrorism financing provisions, many associated threats have moved to the NFT market. A large scale of threats results from imprecise legal regulations on the NFTs. Since each NFT is unique with regard to the linked assets or functions, it can be used on many market segments: from trading in the works of art to the financial services. This lack of transparency in the regulations triggers the gaps in the monitoring system and combating the money laundering and terrorism financing offences.

The NFT transactions pose a threat themselves. This threat covers the conventional frauds, such as NFT transaction forging or misleading the purchasers. This threat is of particular importance on the NFT markets, which operate with the use of automated smart contracts and minimum KYC requirements and

sporadic use of any monitoring mechanisms. However the NFT transactions also feature many threats related to their similarity to the art market. They include anonymity, unregistered sales and involvement of high-risk jurisdiction entities in the transactions. A significant increase in the threat to the transactions occurs when the NFT trading takes place without any intermediaries.

One of the basic sources and methods of financing of ISIL, Al-Quaeda and associated terrorist organisations are the donations of cryptocurrencies via the OTT OTT (Over the Top) application. The attractiveness of this method stems from the fact that the involved virtual currencies enable quick transaction without revealing the "owner's" identity. On-line transactions have the advantage that they enable interactions with the high-risk areas or customers, which cannot be easily identified, even if the transactions remain the identifiable digital tracks in the web. The cryptocurrencies are attractive for the purposes of terrorism financing due to the absence of clear regulations on virtual currencies in many jurisdictions, which also brings the potential opportunities to make safe transactions between the cryptocurrencies and fiduciary currencies. According to the latest *Supranational Risk Assessment* (SNRA), the terrorist groups may be interested in using cryptocurrencies to finance the terrorist activity. The limited, yet growing number of cryptocurrency-related cases have been reported. The Egmont Group detected the cases of terrorist groups using the cryptocurrencies. In this case it is known that these groups have provided instructions concerning the use of cryptocurrencies in the Internet (including via Twitter). The TE-SAT Europol Report for 2020 notices that the number of cases related to the use of cryptocurrencies for the purposes of terrorism financing has remained at a relatively low level. The situation did not change in 2021. The terrorist and extremist groups have more frequently used the crowdfunding methods combined with the use of cryptocurrencies, which was supposed to ensure higher level of anonymity of the donors and beneficiaries. These cases have taken place mostly with regard to Jihad terrorism and extremist right-wing organisations.

The number of signals on the opportunity to use virtual currencies for the purposes of terrorism financing in Poland is low.

Averaged level of threat of the virtual currency sector – ML – 3.0 and FT – 3.0

Averaged level of vulnerability of the virtual currency sector – ML – 3.0 and FT – 3.0

Estimated level of probability for the sector – ML – 3.0 and FT – 3.0

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the virtual currency sector –2.40	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High

3.6 – 4	Very high
ML risk of the virtual currency sector – 2.80	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the virtual currency sector for the purposes of terrorism financing in Poland is at a high level.

CONCLUSION 2: The level of risk of using the virtual currency sector for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the virtual currency sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The business operators involved in the virtual currency sales for cash, in the event of payment with the use of greater volume of cash by the non-EU residence, should reasonably obtain information on the source of origin of assets, for example by verification of the currency declarations of the customers from outside the EU.

The virtual currency sector entities should enhance the activities related to the appropriate assessment of the business relationship of the customer and obtaining information on their purpose and intended nature and should take the actions to enhance on-going monitoring of business relationships. The obligated institutions from the virtual currency sector should put attention to the source of origin of assets of the customers exchanging the virtual currencies, where the exchange virtual currency is the currency of enhanced anonymity.

The currency exchange sector entities should enhance their activities related to appropriate assessment of the executed currency exchange transactions as well as to maintain on-going monitoring of business relationships.

The virtual currency sector should undertake the actions guaranteeing maintenance of high awareness of exposure to the crime of money laundering and terrorism financing, as well as guaranteeing the adequate trainings for the sector staff in the area of analysis of warning signals stemming from the suspicious transactions.

Due to a wide spectrum of operation of the virtual currency sector entities, these entities should make sure that the risk assessment of the entity was adapted to their operation profile and considered the factors and risk specific for the company's activity.

Developing by the virtual currency sector institutions of the advances IT tools and systems supporting the implementation of the anti-money laundering and counter-terrorism financing objectives is recommended.

The trainings for the obligated institutions from the currency exchange sector, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be organised. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended

The obligated institutions should put particular attention to finding data on the source of origin of the transferred funds.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance. The currency exchange sector should put particular attention to the high-volume transactions made with the residents of the jurisdictions in the conflict zones as well as to the transactions indicating that they were executed with the use of an intermediary for the currency exchange purposes.

A significant risk-mitigating factor for the virtual currency sector-related risks at the systemic level should the the adoption and implementation of the solutions provided for in the *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937* and the *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849*. Harmonisation of the approach to the obligations of the virtual currency sector entities at the EU level should limit the currently observed activities coming down to the migration of the entities from the virtual currency sector between the individual jurisdictions from the EU area in order to select the jurisdiction of the requirements best suited for a given entity (by default – the least stringent) with simultaneous maintenance of the right to provide services at the area of the entire Community.

7. Area – telecommunications services linked with mobile payments

Sector description – is contained in sub-chapter 7.2.1 – "Vulnerability of the financial market".

Risk occurrence scenarios (i.e. possible risk occurrence examples) referred to the use of a telecommunications service linked with premium rate numbers for money laundering purposes and the financial products and services in the form of mobile payments for the purposes of terrorism financing. The description of scenarios is presented below.

Money laundering

Table 35

Type of used services, financial products	Telecommunications services linked with premium rate numbers
General risk description	Use of telecommunications services in the area of premium rate numbers to legitimise the proceeds of crime
Risk occurrence scenario (i.e. possible risk occurrence example)	Entering into the agreement for the provision of telecommunication services linked with the registered premium rate numbers for dummy persons (so called straw men) in order to ensure anonymity of the perpetrators. Then, using the relevant codes, the offenders or the associated persons make specific calls for which high payments are collected. A part of earned profit is the payment for the "straw man", while the remaining larger part is used by the offenders as "laundered" money.
Level of vulnerability	4
Justification for the level of vulnerability	Possibility to provide such services and access to them are relatively easy. Hiding the identification data of customers (using the straw men or alternatively foreign phone numbers) is possible. There may be transactions of international nature. These service providers are not the OIs. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information. It is probable that the case of money laundering in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation mostly does not correspond to the scope of the analysed risk.
Level of threat	2
Justification for the level of threat	Using the telecommunications services in the area of premium rate numbers to legitimise the proceeds of crime can be one of the money laundering methods. The GIFI received limited information on the use of such *modus operandi* for money laundering crime, however this method is perceived as unattractive and relatively unsafe. The provider of telecommunications services linked with premium rate numbers is obliged to submit information required by the Act to the register kept by the President of the Office of Electronic Communications[51]. Applying this *modus operandi* requires planning, knowledge and skills. In addition, this method is expensive. CONCLUSION: using the telecommunications services in the area of premium rate numbers to legitimise the proceeds of crime poses a medium threat of money laundering.

[51] https://bip.uke.gov.pl/zgloszenia-do-rejestru-premium/zgloszenia-do-rejestru-premium-rate,1.html

Terrorism financing

Table 36

Type of used services, financial products	Mobile payments
General risk description	Purchasing or topping-up the SIM cards for the purposes of transfer of funds
Risk occurrence scenario (i.e. possible risk occurrence example)	Using mobile payments applying no customer due diligence in the adequate scope for the purposes of terrorism financing in a manner impeding identification of the ordering party and beneficiary of the transactions, for example: the supporters of a terrorist organisation transfer the mobile payments (debiting their phone bills) for one person, who then withdraws the received funds in cash in the ATM to transmit them for the purposes of this terrorist organisation.
Level of vulnerability	4
Justification for the level of vulnerability	Possibility to provide such services and access to them are relatively easy. Hiding the identification data of customers (using the straw men or alternatively foreign phone numbers) is possible. There may be transactions of international nature. These service providers are not the OIs. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information. It is probable that the case of FT in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation mostly does not correspond to the scope of the analysed risk.
Level of threat	1
Justification for the level of threat	Purchasing or topping-up the SIM cards for the purposes of transfer of funds is one of the safest and quick methods of financing of terrorist activities. Using the mobile payment systems, which do not apply customer due diligence in the adequate scope, is cheap and attractive. It is sufficient to enable the option of transfers to the phone number in the mobile app or transfer the funds to the beneficiary for the purposes of withdrawal in the ATM. In Poland, there is no unambiguous information on using this *modus operandi* for the purposes of terrorist activity financing. The obligation of registering the pre-paid numbers in a way that each phone number has a clearly identified user introduced in Poland in 2017 acts as the limitation of anonymity. CONCLUSION: Purchasing or topping-up the SIM cards for the purposes of transfer of funds / collecting funds for the purposes of terrorist activity poses a low threat of terrorism financing.

Table 37

Type of used services, financial products	Telecommunications services linked with premium rate numbers
General risk description	Use of telecommunications services in the area of premium rate numbers to collect funds for the purposes of terrorist activity
Risk occurrence scenario (i.e. possible risk occurrence example)	Entering into the agreement for the provision of telecommunication services linked with the registered premium rate numbers (*Premium* type) for dummy persons (so called straw men) in order to ensure anonymity of the perpetrators. Then, using the relevant codes, the offenders or the associated persons make specific calls for which high payments are collected. A part of earned profit is the payment for the “straw man”, while the remaining larger part is transferred for the purposes of terrorist activity.
Level of vulnerability	4

Justification for the level of vulnerability	Possibility to provide such services and access to them are relatively easy. Hiding the identification data of customers (using the straw men or alternatively foreign phone numbers) is possible. There may be transactions of international nature. These service providers are not the OIs. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information. It is probable that the case of FT in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation mostly does not correspond to the scope of the analysed risk.
Level of threat	2
Justification for the level of threat	Use of telecommunications services in the area of premium rate numbers (PREMIUM services) to collect funds for the purposes of terrorist activity is one of the identified terrorism financing methods. Although in Poland there is no unambiguous information on using this *modus operandi*, the Internal Security Agency (ISA) have recorded the cases of the involved foreigners from the higher risk states in the telecommunications frauds using the PREMIUM numbers in the past, income from which have been most probably allocated to the activity of terrorist groups. For the purposes of financing of terrorist activity, this method is perceived as relative attractive. A dispersed group of supporters or followers of terrorist activities may easily support/credit the provider of telecommunications services linked with premium rate numbers with low amounts. The profits from such activity are allocated to terrorist activity. This *modus operandi* requires planning, knowledge and skills. This method is rather expensive. CONCLUSION: Use of telecommunications services in the area of premium rate numbers (PREMIUM services) to collect funds for the purposes of terrorist activity poses a medium threat of terrorism financing.

Mobile payments are non-cash payments made with a mobile device[52] (e.g. smartphone or tablet) and mobile technologies (e.g. NFC, SMS, USSD, WAP). Mobile devices must be able to connect to the telecommunications network (mobile network or the Internet), while payment is usually made via a bank or payment application. Mobile payments can be divided to:

- contactless – using the NFC technology and applied primarily in the payments in the POS terminals, vending machines, parking meters and toll gates;
- remote – using the Internet connection or GSM technology and applied primarily in the e-stores, between the users (*Peer-to-Peer* – P2P mobile payments), when paying for parking places and urban transport and in the POS terminals to a lesser extent.

The mobile solutions available nowadays enable also cash withdrawals (from the ATMs and cash registers in the form of the *cashback* service), both contactless and remotely. Vast majority of mobile solutions in Poland operates on the basis of payment cards (e.g. Google Wallet, Apple Pay), which enables the use of the opportunities offered by the payment card schemes. For example, in the event of a potential fraud, the aggrieved customers may apply for reimbursement of the lost funds under the *chargeback* procedure. On the other hand, the BLIK system operates on the basis of mobile access to the funds collected directly on the bank account. Modern mobile payments belong to the most secure forms of making payment. Mobile

[52]https://www.nbp.pl/home.aspx?f=/edukacja/zasoby/broszury/platnosci-mobilne.html, access on 23.01.2023

solutions based on the payment cards use tokenization[53] and biometric security measures (for example using the fingerprint, iris or face biometrics to confirm the transactions by the user). Starting from the 2H of 2021, the customers may also use the contactless BLIK payments. A one-off, 6-digit code valid only for 2 minutes is generated on the user's mobile phone screen.

The contactless mobile payments – depending on the devices – can be divided to:

- phone payments – both contactless and in the NFC technology (for example Apple Pay, Google Pay, contactless Blik, HCE) and without this technology (Blik with a code);
- watch payments – this group includes GarminPay and FitbitPay, SwatchPay! and Xiaomi Pay.

According to the study conducted by the Blue Media company, entitled "Finanse Polaków w czasach postpandemicznych 2022" (*Finances of the Poles in the post-pandemic times of 2022*)[54] (study conducted in June 2022) – nearly a half of the Poles (46 %) pays for purchases in the Internet with BLIK. Currently, this is the most frequently selected form of payment, popularity of which has been successively growing for several years. In 2022, BLIK deployed an additional functionality consisting in placing the phone hear the payment card reader only.

The key barriers in using the mobile phones include:

- lack of awareness on the options provided by these payments. The potential users may be unaware of the benefits deriving from such solution;
- use barrier, in effect of which the users do not understand how the technology works and cannot use it;
- lack of awareness of threats posed by using the technology;
- technological barriers, such as attachment to the conventional payment methods and negative perception of technological novelties, in particular among the older recipients.

These factors result in certain reluctance to mobile payments.

A dynamical development of mobile payments is strongly associated with the fears of the society elated to health and health safety. During the COVID-19 pandemic, the World Health Organisation called the consumers for wider use of digital methods of contactless payments in their financial operations. WHO confirmed that the coronoviruses on the banknotes and coins may survive even up to 3 days. Such information was among others the reason to increase the non-cash transaction limits at the territory of a majority of countries in the world, to enable the customers make larger shopping without any limitations and the need to use physical money.

According to the statistical studies, in 2020 nearly a half of consumers aged 18-54 used mobile wallets. The most numerous groups were the Millennials (24-39 years). On the other hand, according to the Cornerstone Advisors[55] study, in December 2020 nearly 80 % of the smartphone owners had at least one mobile payment application installed, provided that the PayPal app was installed on 65% of all smartphones.

[53]Tokenization – data of payment card and specific transaction are replaced by a different digit string i.e. token, which makes them inaccessible to third parties, for example the sellers.
[54]https://bluemedia.pl/baza-wiedzy/badania-i-raporty/blik-metoda-platnosci-deklasuje-inne-220709, access on 23.01.2023
[55]https://mobiletrends.pl/stan-platnosci-mobilnych-kiedys-i-dzis/, access on 23.01.2023

In 2021, the global value of the mobile payment market[56] amounted to nearly USD 2 trillion (2,000,000,000,000 $). According to the estimations, mobile payments are used by a quarter of global population, while the share of their use will increase by another 30% by 2024.

The greatest number of mobile payment users was recorded in China, where as many as 87% of citizens used mobile payments. It is followed by South Korea, which reached nearly 46%. The third place is occupied by the United States with 43%, followed by India with 40%. It should be noted that the Japanese, who have pioneered the deployment of these technologies, were ranked only fifth with the result of 35% of mobile payment users.

The Chinese mobile payment application[57] had the greatest number of users in the world. AliPay is the largest service of this type in the world. Its importance can be evidenced by processing the transaction volume of the total value of USD 17 trillion in 2019. On the other hand, WeChat Pay is a default payment service for WeChat, i.e. the largest Chinese social network service. Outside China, the most popular app in the world is Apple Pay, which has the largest transaction volume.

Vulnerability of the sector

Using mobile payments and telecommunications services in the area of premium rate numbers to legitimise the proceeds of crime as well as access to them are both relatively easy. It is also possible to hide the identification data of the customers (using straw men or alternatively the foreign phone numbers). Transactions of international nature are also possible. The service providers in this sector are not the obligated institutions.

Mobile payments enable both non-cash purchase of various items and services, but also transfer of funds between the accounts. These non-cash payments are made with the use of a mobile device (smartphone, tablet, smartwatch) supported by mobile technologies, such as for example SMS, NFC, USSD and WAP. They also require the connection with a telecommunications network (GSM or the Internet).

The telecommunications services are all services covering the transmission, emission and reception of signals, text, image and sound content or any and form information by cable, radio, optic route or via any other electromagnetic systems. The provision of telecommunications services alone is considered the telecommuncations activity, which requires the entry into the register of telecommunications operators kept by the Office of Electronic Communications – regardless of whether their nature is public o non-public.

During the COVID-19 pandemic there has been an increased interest in mobile payments and the accompanying increase in the value of transactions with mobile payments on the market derived from closing the branches and offices of the financial institutions (or limited business hours). At the same time, this raised the interest in the mobile payment sector both by the offenders and organised crime groups.

The companies involved in the financial technology (FinTech) use the technology to offer the financial services combined with the use of telecommunications services, for example online banking and applications dedicated to mobile payments. According to the "Digital 2021[58]"

[56] Ibidem
[57] Ibidem
[58] https://datareportal.com/reports/digital-2021-global-overview-report, access on 23.01.2023

report, at the turn of the 2020 and 2021 the number of people around the world amounted to 7.83 billion. Nearly half of the population i.e. 5.22 billion is the mobile phone users (not necessarily smartphones). A little less – 4.66. billion, which accounts for 59.5% of the poulation – have used the Internet. Potentially, each smartphone user may use the applications enabling mobile payments. Mobile payments have been already used, for example, by many immigrants and seasonal workers willing to send a part of their earnings home to support their families. Mobile payment transfers have been replacing the conventional services of the banks and companies providing the financial services, which used to impose high charges for low-amount transfers. At the same time, the mobile payments encouraged certain users to avoid using the underground money transfer systems, such as Hawala.

The operation of the operators in the sector concerned may face difficulties related to obtaining from a customer of a wider spectrum of documents confirming the customer's identity or reliability. In Poland, each sold SIM card must be registered under the real name and surname of the purchaser. SIM card registration requires the provision of the Personal ID, and in the case of the company's phones also the National Official Register of Business Entities (REGON) no. or VAT ID. The pre-paid cards without the confirmed identity of the owner lost their validity on 1 February 2017. However, not all countries, even the neighbouring ones, introduced the obligation to register the SIM cards. Sporadic advertisements and specialist e-stores established only for the purposes of selling such cards are available in the Internet. One of them sells the cards of e.g. Czech operators, which will be active without any registration.

The conflict in Ukraine and the presence of a large number of refugees in Poland have raised severe problems with the identification and verification of persons. The existing language and cultural barrier significantly affects proper identification of the increased risk factors. Each refugee may potentially buy a mobile phone and make mobile payments.

Mobile payments create wide opportunities of their use for the purposes of terrorism financing. Development of telecommunications technologies, decreasing the telecommunications and information exclusion (Internet) and rapid expansion of the applications enabling mobile payments have contributed to dynamic development of the financial services, even in the apparently poor developed countries and in the countries of the increased terrorist risk or being the conflict zones or adjoining such zones. In many of them, the financial services have been currently offered via mobile phones. The phone holders may pay their bills, transfer money, receive credits, open the accounts and check balances. Phone can be even used to send remuneration to the employees, not to mention payment by phone for goods and services. Since the funds used for terrorism financing may origin both from legal and illegal sources, the potential funds can be transferred in the form of mobile payments. This is of significance for example when someone arrives to the conflict zones (e.g. Foreign Terrorist Fighters). The fighters may deposit money and withdraw it when arriving to the place of destination or in the neighbouring countries. This procedure is much more effective compared to carrying a large amount of cash. Mobile payments enable avoiding both the conventional banks and the ATMs. Using the applications enabling mobile payments acts potentially as the virtual ATM or wallet for any person, who would decide to finance terrorism with the use of a mobile phone. In addition, in the case of cross-border transactions and involvement of the foreigners, there may be practical difficulties with determination of the place of committing the crime and penal jurisdiction and the competences of the law enforcement authorities in terms of handling the

specific penal proceedings may be challenged. In many cases, the problems with traceability of mobile payments made by phone may arise.

The public administration authorities have basic knowledge on the ML/FT risk in this scope. The General Inspector of Financial Information (GIFI) is not capable to collect and analyse information. It is probable that the case of money laundering or terrorism financing in the scope of the analysed scenarios will not be detected.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation mostly does not correspond to the scope of the analysed risk.

Threats in the sector

In terms of money laundering and terrorism financing threat assessment, the mobile payment sector is the sector that can be potentially used for the predicate offences for the purposes of money laundering and terrorism financing. The new payment methods generate the specific new types of frauds and extortions. The greatest number is still linked to identity thefts (phishing) – as many as 71 % of the sellers identify such frauds[59] – the offenders may take control over a credit card, mobile device (including the SIM card), or a loyalty programme, points from which may be used to make payments. Another fraud is pharming (66 %), consisting in redirecting the user to a false website and taking-over its password, account or credit card data. The objects of these actions are both the users of e-stores and the suppliers, who are attacked by hacker software. In a growing number of cases, these actions take the form of an exchange of false information between the service and the unaware users. There can be also so called "friendly" frauds, when the offenders inform a company that the card used for a transaction was stolen and they ask for reimbursement of funds – thus, the profit covers not only the takeover of the ordered goods or services. Such transaction requires also the data of an intermediary, who/which receives the ordered items, but the fraudsters are focused on money.

The mobile payment services can be used for money laundering or terrorism financing purposes even without establishing the direct business relationships. The business relationships between the supplier and the user of mobile payment services may be established by the agents, on-line or via a mobile payment system. Such threat of mobile payment service anonymisation may be posed by the anonymised products already existing on the market, in particular in the other jurisdictions – including in particular pre-paid cards, which can be connected to the mobile payment services. Verification of the customer's identity may be impeded in such case. Even if the suspicious transaction monitoring and reporting schemes may operate effectively, the absence of effective identification of the mobile payment user may be problematic. It is however the specific financial institutions which decide, whether their cards will be compatible with the mobile payment products, such for example Google Pay or Apple Pay. A specific financial institution may limit the mobile payment options for some or all cards.

The threat in context of money laundering or terrorism financing may also result from the technicalities of mobile payments. Vast majority of mobile payments is based on the banking model i.e. connection of funds on the bank account or mobile card. Certain mobile payment services however do not use the banking model and top up the virtual purse using the other

[59] https://fintek.pl/oszustwa-podazaja-rozwojem-platnosci-mobilnych/, access on 23.01.2023

methods, for example *on-line*, even from an unidentified contractor. Such options to finance the virtual purse obfuscate the origin of the funds, creating the higher risk of money laundering and terrorism financing. One should also consider the fact that the mobile payment users have access to the funds via the international ATM networks. Access to cash via ATMs significantly increases the risk of money laundering and terrorism financing, since it enables transfer of cash in one country and its withdrawal in the other country.

Another threat in context of money laundering or terrorism financing may be a digital smurfing. The users of mobile payment applications can be provided with dirty money and use it for topping-up their mobile phones with a digital value – in accordance with all applicable legal or reporting limits. Then the users of mobile payment applications make multiple transactions of transferring the funds on the accounts controlled by organised crime. In effect of applying such forms of money laundering, the offenders are able to avoid such inconveniences as carrying large volumes of cash and avoid the financial reporting requirements.

Vast majority of the financial intelligence units, including the GIFI, receive no information on financial flows linked with mobile payments. There is no proper analytical modelling of such transactions, which practically prevents their processing and analysing. There are also no practical opportunities of tracking and monitoring of mobile payments, while destructing the evidence in the form of a phone, difficulty to recover or determine the data stored in the phone significantly impedes the investigations conducted by the law enforcement authorities.

Averaged level of threat of the sector of telecommunications services linked with mobile payments – ML – 2.0 and FT – 1.0

Averaged level of vulnerability of the sector of telecommunications services linked with mobile payments – ML – 4.0 and FT – 4.0

Estimated level of probability for the sector – ML – 3.20 and FT – 2.80

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the sector of sector of telecommunications services linked with mobile payments – 2.28	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High

3.6 – 4	Very high
ML risk of the sector of sector of telecommunications services linked with mobile payments – 2.92	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the sector of telecommunications services linked with mobile payments for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the sector of telecommunications services linked with mobile payments for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the sector of telecommunications services linked with mobile payments for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The obligated institutions should scrupulously address the issue of risk assessment of a customer providing the telecommunications services linked with mobile payments, by taking the appropriate mitigating measures and adapting the scope of the applied customer due diligence measures to the profile of customer's activity. At the same time, in the event that may raise doubts, such as significant differences in the volume of payments between the audited periods, it is reasonable to obtain information on the source of origin of the assets from the customer of the obligated institution.

If the customer of the obligated institution uses the solutions enabling payments via payment terminals or payment applications, the factor to be taken into account by the obligated institutions should be the circumstances demonstrating a disproportionately high value of

transactions compared to the profile of business activity of the customer or information about the customer collected to date.

8. Physical cross-border transportation of assets

Sector description – is contained in sub-chapter 7.2.2 – "Vulnerability of the non-financial market", as well as in the chapter 5.3. "The most common methods used to finance terrorism".

Risk occurrence scenarios covered the opportunity to use the natural persons for transportation of cash or other means of store of value (investment metals, precious stones, payment cards, cheques, etc.).

Money laundering

Table 38

Type of used services, financial products	*Cash couriers*
General risk description	Use of natural persons for transportation of illicit proceeds through the state borders
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The natural persons (sometimes hired only for the purposes of one-off transport of assets) transport these assets through the borders in different ways: • one-off transportation of cash below the declaration threshold, • declaration of import/export of cash of the value above the threshold and indicating the fictitious purpose of their us, • transportation/smuggling of cash hidden in luggage, mean of transport, under clothing. 2. Apart from cash, the following assets may be transported: precious stones and metals, works of art, pre-paid cards, cheques, etc. 3. Transportation of high amounts of cash through the borders with simultaneous declaring the import/export of the amount slightly exceeding the threshold required for declarations of foreign currency, which raises no suspicions. The perpetrators hope that the customs or border guard officers will limit their duties to acceptance of declaration and will not look for any other cash of a much higher value transported by the perpetrators.
Level of vulnerability	4
Justification for the level of vulnerability	Access to the asset transportation services is very easy – any person may become a courier. Although during the controls on the external EU borders hiding the identification data of the courier is impossible, the transportation of assets and therefore identification data of the courier can remain unrecognised by the public administration authorities at the border. In the era of the military conflict in Ukraine and acceptance by Poland of the refugees from the conflict zones, crossing the border at the Ukrainian section is strongly facilitated, which potentially enables hiding the identification data of the courier. These service providers are not the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information (information provided by the National Revenue Administration, Border Guard and the Customs Information System). It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4

Justification for the level of threat	The use of natural persons for transportation of cash through the state borders is one of the most common methods of money laundering. Transportation of cash or other assets through the state borders is a widely available method and its use is relatively inexpensive and is perceived by the perpetrators as attractive and relatively safe, the more when the transported amounts are below the threshold of an obligatory import declaration. The use of natural persons for transportation of cash through the state borders requires neither specialist knowledge on the banking system, nor specialist skills and ensures anonymity of the group/organisation supervising this process. The GIFI has received information on the possibility to use this method for money laundering purposes. The Polish services have recorded the cases of using this method for transfer of cash between the participants of money laundering process. CONCLUSION: Use of natural persons to transfer the illicit proceeds through the state borders poses a very high threat of money laundering.

Table 39

Type of used services, financial products	Courier parcels, postal parcels, cargo shipments
General risk description	Use of courier and postal services to transfer the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	An offender transfers the illicit proceeds in the parcels sent by post to the natural persons staying in the other countries. The funds recipients introduce them to the financial system (for example by crediting the bank accounts) for the purposes of investments or using these funds to purchase the goods which are then made available to the offenders.
Level of vulnerability	3
Justification for the level of vulnerability	Access to the courier and postal services and cargo shipments is relatively easy. It is possible to hide the identification data of the parcel senders and recipients. The courier and postal parcels as well as the goods shipped with cargo are transferred between the persons and entities from various countries. In the era of the military conflict in Ukraine, is is potentially possible to use the identification data of the persons from the conflict zones, which have been occupied by the enemy or destroyed during warfare. Only a part of these service providers is the OIs. This excludes the carriers and forwarding companies. The public administration authorities have limited knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information (only in a limited scope). It is highly probable that the case of money laundering in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation only partially corresponds to the scope of the analysed risk.
Level of threat	3

Justification for the level of threat	The use of courier and postal services to transfer the illicit proceeds is a relatively easy and widely available method of money laundering and its use is relatively inexpensive. It is perceived by the perpetrators as rather attractive. Using the courier or postal services usually raises no suspicions. A high turnover – in terms of international consignments – enables hiding the use of these services for money laundering purposes. "Straw men" are frequently used to hide the beneficial owner. In the era of the military conflict in Ukraine it is easy insofar as there are problems with identification and verification of a part of the refugees. These persons, when crossing the border, either had no documents, or their documents had the form of an internal passport in Cyrillic. Using this *modus operandi* requires however planning, knowledge about the shipping system and logistic skills. The GIFI has received information on the use of this method for money laundering purposes, in particular in combination with the other methods. CONCLUSION: Use of courier and postal services to transfer the illicit proceeds poses a high threat of money laundering.

Terrorism financing

Table 40

Type of used services, financial products	Cash couriers
General risk description	Use of natural persons for transportation of illicit proceeds through the state borders
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The natural persons (sometimes hired only for the purposes of one-off transportation of assets) transport these assets through the borders in different ways: • one-off transportation of cash below the declaration threshold, • declaration of import/export of cash of the value above the threshold and indicating the fictitious purpose of their us, • transportation/smuggling of cash hidden in luggage, mean of transport, under clothing. 2. Apart from cash, the following assets may be transported: precious stones and metals, works of art, pre-paid cards, cheques, etc. 3. Transportation of large values of cash through the borders with simultaneous declaring the import/export of the amount slightly exceeding the threshold required for declarations of foreign currency, which raises no suspicions. The perpetrators hope that the customs or border guard officers will limit their duties to acceptance of declaration and will not look for any other cash of a much higher value transported by the perpetrators.
Level of vulnerability	4
Justification for the level of vulnerability	Access to the asset transportation services is very easy – any person may become a courier. Although during the controls on the external EU borders hiding the identification data of the courier is impossible, the transportation of assets and therefore identification data of the courier can remain unrecognised by the public administration authorities at the border. In the era of the military conflict in Ukraine and acceptance by Poland of the refugees from the conflict zones, crossing the border at the Ukrainian section is strongly facilitated, which potentially enables hiding the identification data of the courier. These service providers are not the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information (information provided by the National Revenue Administration, Border Guard and the Customs Information System). It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.

Level of threat	4
Justification for the level of threat	The use of natural persons for transportation of cash through the state borders is one of the most common methods of financing the terrorist activity. Transportation of cash or other assets through the state borders is a widely available method and its use is relatively inexpensive and is perceived by the perpetrators as attractive and relatively safe, the more when the transported amounts are below the threshold of an obligatory import declaration. The use of natural persons for transportation of cash through the state borders requires neither specialist knowledge on the banking system, nor specialist skills and ensures anonymity of the group/organisation supervising this process. The GIFI has received very little information on the possibility to use this method for terrorism financing purposes. The Polish services have recorded the cases of using this method for transfer of funds intended for terrorist activity. CONCLUSION: Use of natural persons to transfer the illicit proceeds through the state borders poses a very high threat of terrorism financing.

Table 41

Type of used services, financial products	Courier parcels, postal parcels, cargo shipments
General risk description	Use of courier and postal services
Risk occurrence scenario (i.e. possible risk occurrence example)	A supporter of a terrorist organisation transfers money collected for the purposes of this organisation in the parcels sent by post to a natural person living in one of the countries neighbouring the area of activity of the terrorist organisation, who then provides the received funds to the members of this organisation.
Level of vulnerability	4
Justification for the level of vulnerability	Access to the courier and postal services and cargo shipments is relatively easy. It is possible to hide the identification data of the parcel senders and recipients. The courier and postal parcels as well as the goods shipped with cargo are transferred between the persons and entities from various countries. In the era of the military conflict in Ukraine, is potentially possible to use the identification data of the persons from the conflict zones, which have been occupied by the enemy or destroyed during warfare. Only a part of these service providers is the OIs. This excludes the carriers and forwarding companies. The public administration authorities have limited knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information (only in a limited scope). It is highly probable that the case of FT in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation only partially corresponds to the scope of the analysed risk.
Level of threat	3
Justification for the level of threat	The use of courier and postal services to transfer money to the terrorist organisations for the purposes of terrorist activity is one of the identified methods of terrorism financing. It is a relatively easy and widely available method of money laundering and its use is relatively inexpensive. It is perceived by the perpetrators as rather attractive. Using the courier or postal services usually raises no suspicions. A high turnover – in terms of international consignments – enables hiding the use of these services for transferring money terrorist activity purposes. "Straw men" are frequently used to hide the beneficial owner. In the era of the military conflict in Ukraine it is easy insofar as there are problems with identification and verification of a part of the refugees. These persons, when crossing the border, either had no documents, or their documents had the form of an internal passport in Cyrillic. Using this *modus operandi* requires however planning, knowledge about the shipping system and logistic skills.

	The GIFI has received very little information on the use of this method for terrorist activity financing purposes. CONCLUSION: Use of courier and postal services to transfer money to the terrorist organisations for the purposes of terrorist activity poses a high threat of terrorism financing.

Transportation of such funds may refer to the export of illicit proceeds for the purposes of their hiding or their import to the country for their investing or financing the illegal activity. In terms of terrorism financing, the options of import to the country of the funds which could be used for financing the attacks, or export of such funds collected from the supporters in the country to finance the terrorist activity at the territory of the other states can be considered. The possible risk covers also the possibility of using the territory of the country to transit such funds.

Annex I to the 2022 SRNA document indicates that the supervision over the funds moved outside the territory of the EU, which may be used to finance the terrorist and military activities in the third countries is of particular importance. This applies in particular to the fighters arriving to the battle zone, who additionally carry with them the funds for own living purposes and for financing the activity of the organisation. Such amounts frequently fall within the range of the permitted transit limits specified by law. The annex notices also that the most convenient method from the perspective of the perpetrators is using the postal or courier services, which reduces the probability of heading the courier off.

In terms of money laundering, transportation of cash is a recognised logistic method of movement of illicit proceeds due to the cash nature of settlements for a significant part of illegal activities. Using the high-denomination banknotes is of particular importance here. The offenders using cash transactions need to relocate the collected funds to the location, where they are safe, or may be (due to the existing control system or market conditions) easier introduced to legal trading. Using the couriers is important in so far that they are exploited in even in the offenses which generate only minor trading in cash, for example ATM or BLIK frauds, where the "dummy persons" collect cash gained from cybercrime. The volume of trading in cash from illegal activities is estimated even for a billion dollars a year.

The rules of transiting the foreign or national currencies through the state border of Poland are governed by the provisions of the *Act of 27 July 2002 – Foreign Exchange Law.* Transportation of cash above EUR 10,000 is subject to declaration, regardless of whether the funds are imported or exported. Cash includes both banknotes and circulation coins, bearer-negotiable instruments, including traveller's cheques, bills of exchange etc., goods used as highly liquid mean of store of value, pre-paid cards, banknotes and coins other than the official legal tenders in the country, which may be however convertible into the circulation currency as well as FX

gold and platinum. These rules do not apply to cash transited through the internal borders of the Schengen Zone[60].

Vulnerability

Annex I to the Supranational Risk Assessment indicates the cash couriers' activity as one of the major sectoral threat. The scale of the problem is evidenced by the fact that during the joint action of the law enforcement authorities from 25 countries in the world supported by Europol, Interpol, Eurojust and the European Banking Federation carried out between September and November 2022, as many as 2469 couriers (originally: money mules) and 22 recruiters were arrested. In effect of the action, 4089 illegal transactions were identified and EUR 17.5 million were intercepted[61].

During the COVID-19 pandemic and related movement restrictions, this phenomenon has been significantly reduced. Resuming the controls on the internal Schengen borders and long lockdown periods have impeded or even prevented a free and unlimited transportation of cash. Regression of the crisis and abolition of the restrictions enabled resuming the use of this method of transfer of funds. In addition, the inflow of refugees triggered by the outbreak of war in Ukraine resulted in the increased risk of inflow of illicit proceeds. A part of the persons crossing the border was no subject to a complete border check, even though that in many cases they have carried a significant volume of personal property. When combined with the impeded process of personal data verification, it is clear that the possibility of inflow of unregistered funds and other assets has increased, the more that Poland has accepted the largest number of the refugees.

The competent state authorities certainly have relevant knowledge and awareness of the presence of threat. The GIFI receives information on the confirmed attempts of transportation of cash through the border. In the event of detecting the transportation, sentencing a direct perpetrator is highly possible. The negative feature of this process is the fact that penalising the actual organiser or ordering party is less probable compared to penalising the courier.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector.

The fact that the physical transportation of cash is an entirely unregulated market poses a major threat. Vast majority of persons operating on this market are the natural persons, who do not operate as business entities. This results from the essence of such activity, which is supposed to be used for transportation of illicit proceeds. Transportation is performed covertly, and its potential detection depends only from the effectiveness of the police forces and border services. Thus, the operational and control activities are the only tools to monitor and control this phenomenon.

From the AML/CFT perspective, transportation of cash or means of store of value is one of the most significant sources of risk, since it forms an essential part of cash trading and the

[60]https://granica.gov.pl/j/index.php/535; access on: 16.12.2022,

[61]2 469 money mules arrested in worldwide crackdown against money laundering | Europol (europa.eu); access on 15.12.2022

processes, without which it would be impossible. It can be assumed that each type of illegal activity, in which cash is involved, will result in the need for its transportation sooner or later.

In terms of terrorism financing, one should note that Poland has recorded the cases of supporting the foreign fighters groups. There are organised groups of supporters of various foreign organisations operating in the country, which frequently refer to violence. There is an actual risk of using this background for the purposes of financing the terrorist activity outside the country[62]. The couriers transporting the assets abroad may undoubtedly form a part of this process.

The opportunity of transportation of non-registered assets within the Schengen Zone is also created by making use of the existing or still unidentified gaps in the Polish financial system for the purposes of money laundering.

The technical issue is the logistics linked with the collection and transfer of funds, which must include collection of cash or assets from the sources on one hand, and coordinated handover to the appropriate persons or entities responsible for legalisation in the European Union or movement to the third country on the other hand. Development of the adequate structure is impeded in particular in the case of comprehensive and profitable types of illegal activity, for example drug trafficking or prostitution. However in vast majority of cases, transportation does not apply to large volumes of cash and is potentially easy to organise. Organisation of transportation requires no specialist knowledge.

Averaged level of threat of the sector of physical cross-border transportation of assets – ML – 3.5 and FT – 3.5

Averaged level of vulnerability of the sector of physical cross-border transportation of assets – ML – 3.5 and FT – 4.0

Estimated level of probability for the sector – ML – 3.50 and FT – 3.80

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the sector of physical cross-border transportation of assets – 2.88	
1 – 1.5	Low
1.6 – 2.5	Medium

[62] The Chechens accused of supporting terrorism did not help the Islamic State – said the expert witness before the court in Białystok (radio.bialystok.pl), access on: 19.12.2022

2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the sector of physical cross-border transportation of assets – 3.10	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the physical cross-border transportation of assets for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the physical cross-border transportation of assets for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the physical cross-border transportation of assets for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The obligated institutions should put particular attention to the foreign exchange transactions linked with the jurisdictions of higher money laundering and terrorism financing risk. The obligated institutions should put particular emphasis on the identification of data on the source of origin of transferred funds and documents justifying a given transaction. In the event or exchange or payment of a greater amount of cash by the non-EU residents, the obligated institutions should consider requesting the customer to present information on the source of origin of assets, e.g. by requesting the customers from the non-EU states to present a copy or confirmation of submitting the declarations of foreign currency.

The obligated institutions accepting the payments or cash deposits in foreign currencies should verify the source of origin of assets, including acquire information from the customer confirming the foreign exchange or submitting the declarations of foreign currency as a reasonable measure.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. The obligated institutions should put particular focus on high-value cash transactions made with the residents of the jurisdictions in the conflict zones as well as on the transactions indicating the use of an intermediary for the foreign currency exchange purposes.

At the systemic level, it is reasonable to take the actions aimed at enhancing the state border protection system against the illegal flow of cash. Introduction of a viable penalty for failure to report transportation of cash through the border would be a highly reasonable solution. Improving the schemes of retention of the illegally transported assets and their potential confiscation should be also considered.

9. Area – gambling

Sector description – is contained in sub-chapter 7.2.1 – "Vulnerability of the financial market".

Risk occurrence scenarios (i.e. possible risk occurrence examples) referred to the use of online gambling for money laundering purposes; use of betting for legitimisation of the illicit proceeds; use of casino gambling for the obfuscation of the origin of funds; buying the winning tickets for the illicit proceeds and using the online gambling scheme for terrorism financing. The description of scenarios is presented below.

Money laundering

Table 42

Type of used services, financial products	Online gambling
General risk description	The illicit proceeds are laundered with the use of online gambling
Risk occurrence scenario (i.e. possible risk occurrence example)	Using the online gambling platforms for laundering of the illicit proceeds, such as from frauds. In the course of analysis of the notifications from the obligated institutions and information from the foreign partners, the GIFI identified the following practice: 1. An offender opens an account on the gambling platform on the basis of false or stolen identification data or takes the control over the existing account kept for the other entity. 2. The offenders "hacked" the credit cards and laundered the funds stolen from these card accounts using online gambling for the purpose of transferring these funds for the organisers of this practice. 3. Using the online gambling platforms for laundering the illicit proceeds, such as from frauds. 4. An offender deposits the funds using among others cryptocurrencies, funds collected on a bank account, credits from payment cards (frequently on the basis of stolen data), anonymous pre-paid cards or transfers of money on a dedicated account linked to a gambling platform. 5. The funds are used for low-risk gambling or alternatively used for gambling purposes in so called chip dumping process – one of many gamblers intentionally loses to the other "dummy" gamblers, purposefully transferring the funds onto the accounts of the other participants. 6. The funds in the form of a "win" are withdrawn from the account linked to a gambling platform by means of money transfers, transfers onto the bank accounts or are exchange to virtual currencies.
Level of vulnerability	2
Justification for the level of vulnerability	Access to online gambling is relatively easy due to the new gambling domains appearing in the Internet on a regular basis. The licence issued by the other state does not legalise the gambling activity in Poland. In the case of the foreign online casinos, hiding the identification data of the player is easy. It is possible to make transactions of international nature, including in particular in the case of financial transactions, when the accounts of the online gambling provider are located abroad. Notwithstanding the above, the National Revenue Administration (NRA) in cooperation with the Polish Financial Supervision Authority (PFSA) drawn up the rules on how to restrict the use of payment instruments or services offered by the payment service providers in Poland for the purposes of transactions linked with illegal gambling. The hosting service providers delete/block access to the prohibited content related to illegal online gambling. Gambling via Internet, excluding betting and promotional lotteries, is covered by the state monopoly. According to Polish law, Poland hosts only one legal online casino. This is the Total Casino established in 2018 and owned by the state company - Totalizator Sportowy. The payments in this casino are enabled by wire transfers, Visa, Dotpay or BLIK.

	All legal gambling providers are the obligated institutions (OIs). Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. According to analysis of information received by the GIFI, the value of funds that can be laundered by a given entity by means of online gambling is – in unit terms – low due to the restrictions imposed by the business entities involved in such activity and the mechanisms enabling identification of the linked accounts potentially used for illegal activities. The public administration authorities have limited knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It receives also spontaneous information from the foreign partners concerning the suspicious transactions reported by the foreign online casinos, which is related to Poland and the Polish citizens. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2
Justification for the level of threat	Use of online gambling may be one of the methods of the illicit proceeds laundering. Pursuant to the Polish legislation however, gambling via Internet, excluding betting and promotional lotteries, is subject to the state monopoly. The regulations prohibit both online gambling by the non-licensed entities and participation in such gambling. The control activities of the NRA, establishment of the Register of online gambling domains non-compliant with the act and blocking access to the prohibited online domains may negatively affect the possibility of using the illicit proceeds. The GIFI has received information on the possibility of using this *modus operandi* in Poland, by way of using online gambling for money laundering purposes. This method, due to legal regulations, seems to be perceived by the perpetrators as unattractive and relatively risky, to legitimise the illicit proceeds. In addition, this *modus operandi* requires planning, knowledge and skills. CONCLUSION: Use of online gambling for the illicit proceeds laundering poses a medium threat of money laundering.

Table 43

Type of used services, financial products	Betting
General risk description	Use of betting for legitimisation of the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	An offender, anticipating the results of sports events, makes a bet at a bookmaker using the illicit proceeds (frequently – to increase the chances to win – by diversifying the bets and allocating the funds to various bets for various sports events). The wins are its legal profit, confirmed by a bill received from a bookmaker.
Level of vulnerability	2
Justification for the level of vulnerability	Access to betting is relatively easy. There are two basic forms of bookmaking companies operating on the market: so called ground bookmakers i.e. the companies having the stationary points (proverbial "counters"), in which the customer pays with cash or card and receives a ticket and so called online bookmakers operating in the web. Hiding the identification data of the illegal gambler is relatively easy, in particular when using the online payment platforms of the foreign operators. The legal bookmakers apply the adequate customer due diligence measures. It is possible to make transactions of international nature, in particular with a view to financial transactions, where the accounts of the online gambling provider (foreign operator) are located abroad. According to the

	estimations of the Ministry of Finance, the "gray market" in the online betting sector in amounted to 9.2% in 2021 (decrease by 1.2% compared to 2022). The share of gray market in betting in Poland in 2021 is below the EU average.[63] All legal gambling providers are the OIs. Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	Use of betting for legitimisation of the illicit proceeds is one of the frequently used money laundering methods. False win statements are the documents, which may contribute to legitimisation of the proceeds of crime. This method is relatively easy, widely available and requiring only moderate specialist knowledge. Using this method is relatively inexpensive and perceived by the perpetrators as rather attractive. The offenders, when choosing this *modus operandi*, in many cases illegally affect the results of the events they bet, for example sports (or other) events. Using this *modus operandi* requires however planning, knowledge about the rate setting (or affecting the correctness of estimation of occurrence of a given event by a bookmaker). The GIFI has received information on using this method for money laundering purposes. CONCLUSION: Use of betting for legitimisation of the illicit proceeds poses a high threat of money laundering.

Table 44

Type of used services, financial products	Casino
General risk description	Use of casino gambling for the purposes of obfuscation of the origin of funds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. An offender buys chips in the casino, for example for cash. After using a small part of them, the offender exchanges the chips back to cash. 2. When playing poker, one of the offenders intentionally loses the chips purchased for illicit proceeds to a linked person, who then exchanges the chips to cash.
Level of vulnerability	2
Justification for the level of vulnerability	Access to gambling (including online) is relatively easy. The legal gambling centres keep the records of visitors. Registration is necessary to access the gambling centre. Although hiding of identification data of a gambler in the Internet is easy, the online payments need to be made from the account of a registered person and may be also credited back on the account of the registered person. In the only legal Polish online casino, playing poker is enabled only with a croupier. The foreign casinos enable gambling with the other persons, however participating in online gambling having no applicable licence at the territory of Poland is illegal and forms a tax petty offence or offence.

[63] https://www.gov.pl/web/finanse/sytuacja-na-rynku-gier-hazardowych-online

	If a gambler participates in the illegal casino gambling, such gambler is able to make transactions of international nature, in particular if the accounts of the online gambling provider are located abroad. All legal gambling providers are the OIs. Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Use the casino gambling for the purposes of obfuscation of the origin of funds is one of the most comprehensively described methods of money laundering. The only legal online casino in Poland is managed by the Totalizator Sportowy Sp. z o. o. Use of casino gambling is a widely available method, its use is relatively inexpensive and perceived by the perpetrators as very attractive. Use of casino gambling for the purposes of obfuscation of the origin of funds requires neither specialist knowledge on the casino itself, nor specialist gambling skills. The method is frequently used by the organised crime, in some cases linked with corruption of the casino staff. The customer due diligence measures implemented by the casinos are skipped in this *modus operandi* by corruption of the casino staff or document forgery. The win statements issued by the casino are valid documents confirming the legal nature of funds held by the offenders. CONCLUSION: Use of casino gambling for the purposes of obfuscation of the origin of funds poses a very high threat of money laundering.

Table 45

Type of used services, financial products	Games of chance
General risk description	Buying the winning tickets for the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	A perpetrator, acting in collusion with a person involved in managing the games of chance, identifies the winners of these games. Then the perpetrator buys back the winning tickets from them.
Level of vulnerability	2
Justification for the level of vulnerability	Access to the games of chance is relatively easy. It is easy to hide the identification data of the gambler, in particular when paying for the ticket in cash. All legal gambling providers are the OIs. Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2

Justification for the level of threat	Buying the winning tickets for the illicit proceeds may be one of the methods of money laundering. The GIFI has received very little information on using such *modus operandi*, however this method is perceived as unattractive and relatively unsafe. An entity making payments from the games of chance or betting provides no access to the list of the winners, which implies the need to reach them. It is also expensive due to the 10% tax on winnings, which additionally increases the costs of using this method. This *modus operandi* requires planning, knowledge and skills. CONCLUSION: Buying the winning tickets for the illicit proceeds poses a medium risk of money laundering.

Terrorism financing

Table 46

Type of used services, financial products	Online gambling
General risk description	The illicit proceeds acquired for the promotion of terrorism were laundered by means of online gambling
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The offenders "hacked" the credit cards and laundered the funds stolen from these card accounts using online gambling for the purpose of using them for payments for the websites promoting the fight and "martyrdom" of the terrorists, which have been also used for contacts between the terrorists and exchanging information on the bomb production methods. 2. Using the online gambling platforms for laundering of the illicit proceeds, such as from frauds. A supporter of a terrorist organisation deposits the funds on the account linked to a gambling platform. The funds are then transferred back to the platform customer concerned as a "win" and then used for terrorism financing purposes.
Level of vulnerability	2

Justification for the level of vulnerability	Access to online gambling is relatively easy due to the new gambling domains appearing in the Internet on a regular basis. The licence issued by the other state does not legalise the gambling activity in Poland. In the case of the foreign online casinos, hiding the identification data of the player is easy. It is possible to make transactions of international nature, including in particular in the case of financial transactions, when the accounts of the online gambling provider are located abroad. Notwithstanding the above, the National Revenue Administration (NRA) in cooperation with the Polish Financial Supervision Authority (PFSA) drawn up the rules on how to restrict the use of payment instruments or services offered by the payment service providers in Poland for the purposes of transactions linked with illegal gambling. The hosting service providers delete/block access to the prohibited content related to illegal online gambling. The first (legal) online casino was established in Poland in 2018. According to the Act, the only company entitled to provide such services online is Totalizator Sportowy. The payments in this casino are enabled by wire transfers, Visa, Dotpay or BLIK. All legal gambling providers are the obligated institutions (OIs). Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfillment are still revealed. Compared to the other OIs, the gambling business entities provide relatively little information on the suspicious transactions/activity. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1
Justification for the level of threat	Use of online gambling may be one of the methods of using the illicit proceeds for the purposes of terrorism financing. Pursuant to the Polish legislation however, gambling via Internet, excluding betting and promotional lotteries, is subject to the state monopoly. The regulations prohibit both online gambling by the non-licensed entities and participation in such gambling. The control activities of the NRA, establishment of the Register of online gambling domains non-compliant with the act and blocking access to the prohibited online domains may negatively affect the possibility of using the illicit proceeds forr the purposes of terrorism financing. The GIFI has received no information on the possibility of using this *modus operandi* in Poland, by way of using online gambling for terrorism financing purposes. This method, due to legal regulations, seems to be perceived by the perpetrators as unattractive and relatively risky, to legitimise the illicit proceeds. In addition, this *modus operandi* requires planning, knowledge and skills. CONCLUSION: Use of online gambling for the illicit proceeds laundering poses a medium threat of terrorism financing.

The legal basis for the operation of the gambling market in Poland is the *Act on gambling of 19 November 2009,* as amended, including the key amendment for this market of 15 December 2016. The gambling market in Poland is a regulated market and is not governed by the Community legislation. The EU gambling market is governed by the subsidiarity principle. For the gambling market this means that pursuant to this principle, the member states may independently develop the provisions on gambling at their respective territories. This includes access to the market, tax issues and the protection of gamblers.

A vast majority of segments of the global gambling market are the regulated market with access restrictions (by the concession, licence or permit systems). Due to social sensitivity of

gambling, the supervisory authority attempt to control the demand by means of this system, to having the protection of gamers in mind. The protection of gamers (as the citizens of a specific state) involves frequently entrusting the gambling of the highest risk of addiction to the state authorities. This includes machine gaming or online games of chance. The state monopoly in certain segments is also frequent on the global gambling market. In most cases, the monopoly covers the numeric games and cash lotteries.

The inherent feature of practically each gambling market in the world is the division of this market to so called white, gray and black market. We speak about white (legal) market, when the operator holds an appropriate concession, licence or permit for the organisation of gambling or betting in the same jurisdiction, in which the gambler is located. The gray market is when the operator holds a licence on the other national market than the market, in which the player is located. The black (illegal) market occurs, when the gambling operator has no licence for any jurisdiction. Depending on a specific jurisdiction, the definitions of illegal activity may certainly differ, with a focus on various elements related to the gambling market. Taking the specific elements of the Polish gambling market into account, it can be stated that practically there are no present active black market segments. Apart from the market belonging to the legal operators, there is rather only gray market present in Poland. This is linked to the fact that the companies being the gambling operators and present in the gray market have no difficulties with establishing the legal undertakings for example in Malta and providing gambling services to the Polish customers. According to many opinions, the black gambling market in the continental Europe is rather negligible and focused mainly on the US, Asian and Australian markets.

As noted in the Supranational Risk Assessment[64] (SNRA), the gambling sector features a dynamic economic growth and technological development, despite the projected drop in 2020 and 2021 due to crisis caused by the COVID-19 pandemic. This document estimates the total revenue from gambling in Europe for EUR 75.9 billion in 2020 (23% drop compared to EUR 98.6 billion of gross revenue from gambling in 2019). Revenue from online gambling in the EU and United Kingdom was estimated for approx. EUR 26.3 billion in 2020 compared to EUR 16.5 billion in 2015. Revenue from offline/stationary gambling also decreased from approx. EUR 77.5 billion in 2015 to approx. EUR 49.6 billion in 2020 due to closures of the stationary gambling centres during the COVID-10 pandemic crisis.

In Poland, participation in the illegal gambling constitutes a tax offence[65]. This applies also to the participation in foreign gambling or gambling organised or carried out in contrary to the *Act of 19 November 2009 on gambling* or terms and conditions of the concession or permit. This offence is subject to fine up to 120 daily rates.

A participant of the illegal gambling is also subject to a financial penalty of 100% of win including the paid stakes. The only legal participation is in the gambling organised by the entities holding the permit on the domains listed on the official website of the Tax Portal.

Vulnerability of the sector

[64] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorism financing affecting the internal market and relating to cross-border activities; {SWD(2022) 344 final}

[65] https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/rejestr-domen/, access on 26.01.2023

Under the AML/CFT Act, all operators in the area of games of chance, betting, card games and machine gaming in the meaning of the *Act of 19 November 2009 on gambling* are the obligated institutions. This obliges them to apply the customer due diligence measures in each case of stake betting and receiving the wins of equivalence of EUR 2,000 or more, regardless of whether the transaction is made as a single or several operations, which seems to be interlinked.

The customer due diligence measures listed in the Act cover primarily the activities the activities related to the identification of a customer and verification of its identity; identification of the beneficial owners and taking reasonable activities to verify its identity. In addition, the a/m obligated institutions check the sources of origin of assets being at the customer's disposal in the situations justified by the circumstances, monitor the customers on the on-going basis and monitor their transactions to identify the suspicious transactions.

In effect of COVID-19 pandemic and establishment of many restrictions, orders an bans due to the outbreak of pandemic between 2020 and 2021, a major surge of illegal activity in the area of gambling has been noticed. A large part of the gambles is unaware that they participate in the illegally organised gambling (usually at the foreign operator). They have also no knowledge on how to find a legal operator, since according to the legislation in force there is no sufficient information on such operators in public domain.

When assessing the level of vulnerability of the system in the area of gambling, one should take into account the potential opportunities of infiltration or takeover by the organised crime groups of the market operators or intermediary companies, by the agency of which these operators conduct their activity on the market. The lowest risk of infiltration of the gambling market operator or the intermediary in the sales of gambling services is in the situation of the state monopoly on a specific market. Covering the gambling market operators with the system of regulation of business activity, performance of which requires compliance with certain conditions provided for by law, is also of a great importance.

In the survey distributed by the GIFI in August 2021 to the obligated institutions and cooperating units, with the request to indicate (maximally) 5 products and services offered outside the financial market, which are or can be most frequently used for money laundering, online gambling was ranked among the 5 products and services most frequently mentioned both by the cooperating units and the obligated institutions. The online gambling market in Poland is a regulated market. Pursuant to Article 5(1b) of the *Act on gambling* organisation of gambling via Internet, excluding betting and promotional lotteries, is covered by the state monopoly. The only legal online casino is the Total Casino, supervised by the Totalizator Sportowy. Total Casino enables such payment methods as: Dotpay, BLIK, payment cards and bank transfer. In addition, Total Casino accepts payments only in PLN. In order to protect the online gambling market, the minister competent for finance keeps the Register of domains offering gambling services in contrary to the Act. The Register is open and data contained in the Register are accessible for everyone. The entry into the Register includes the name of online domain used for gambling purposes or name of domain used to advertise or promote gambling in contrary to law, accessible to the Internet users at the territory of the Republic fo Poland.

With the view to the existing provisions of the *Act on gambling*, the stationary casinos may be run by private entities – the operation of the casinos is however licensed. The licence, awarded for the period of 6 years may be applied for only by the limited liability companies or joint stock companies of share capital of at least PLN 4 million, against which no justified

reservations from the perspective of state security, public order, state economic interest security as well as compliance with the regulations governing anti-money laundering and countering the financing of terrorism can be brought. In addition, the entities willing to operate a casino – subject to compliance with the statutory conditions – must also take part in the tender announced by the Minister of Finance, provided that the licence for a given location is applied for by more than one entity. The permissible number of stationary casinos depends on the geographic and social conditions. The number of stationary casinos is determined on the basis of the population number – one casino per area inhabited by less than 250 thousand people, and the number of casinos may be increased proportionally by one per each subsequent 250 thousand. However, the total number of gambling casinos per voivodeship cannot exceed 1 casino per 650 thousand of the voivodeship population in total. In practice, the stationary casinos are characterised by low vulnerability to money laundering or terrorism financing. The licensed stationary casinos apply customer due diligence, store data, and each person entering the casino is photographed. Thanks to this, the casino staff is aware, who entered the casino and in what time, what identity document was presented by this person and how did such person look like. This enables proper identification, even if a given person uses one or several false identity documents. The casinos use for example the face recognition software. The CCTV systems in the casino cover not only the gambling premises, but also the other key areas of activity. All transactions made in the casinos are monitored and documented. It is important that the amounts of cash that could potentially be laundered in the casino, are strictly limited due to the fact that any large volume of cash would immediately alert the casino staff. In addition, even a request for issuing the win statement itself triggers the verification activities on the course of gambling of the requesting person, which is carried out by the casino staff.

Machine gaming allowed only in the amusement arcades. Running these arcades is the responsibility of the Totalizator Sportowy (at the end of 2020, there were more than 5000 amusement arcades operating, while as of the end of 2021 nearly 900). The amusement arcades are subject to restrictions, such as: obligation of gambler registration; location requirements for the amusement arcades – no more than 1 room per 1000 inhabitants of the poviat; time and amount limits for machine gaming; requirement of keeping the central system recording the events in real-time; requirement of keeping the audiovisual system; arcade certification system; jackpot ban.

Betting is a regulated activity and may be organised by the private entities operating in the form of a limited liability activity or a joint-stock company. The provisions provide also for the requirement of minimum amount of share capital of the company (operator), which for the bookmaking sector operators was set at the level of PLN 2,000,000. The permit of the Minister of Finance for betting is obtained by the entities separately for stationary betting shops and separately for organisation and running the activity in the area of betting via Internet. In order to protect the betting market, the a/m register of domains used to offer gambling services in contrary to the Act and kept by the Minister of Finance, was established.

A legal part of the online casino and bookmaking sector[66] generated the turnover of PLN 26.6 billion in this time, while the legal stationary market operators reached the turnover of PLN 7.4

[66] https://www.isbtech.pl/2022/12/raport-ey-szara-strefa-w-branzy-hazardowej-online-to-juz-ponad-50/, access on 26.01.2023. According to the report of the EY consulting company prepared for the "Graj Legalnie" (Gamble Legally) association, the turnover generated in the gray online gambling market in Poland amounted to PLN 27.7

billion (PLN 1.5 billion by bookmakers and PLN 5.9 billion by casinos). Thus, the turnover value of the entire casino and bookmaking market in Poland reached PLN 61.7 billion, excluding the gray market on the stationary market.

Supervision over compliance with law of the gambling operators performed by means of the customs and tax controls is carried out by the Minister of Finance and the National Revenue Administration authorities. The basis for gambling market controls is the *Act of 16 November 2016 on the National Revenue Administration* (Journal of Laws of 2023, item 615). The tasks of the National Revenue Administration include the customs and tax control in the area of gambling and identification, detection, prevention and countering the tax offences and petty offences against organisation of gambling and prosecution of their perpetrators. The NRA tasks include also the tax controls in the area of gambling and surcharge tax. In total, in 2021, the NRA authorities performed 1,004 customs and tax controls[67] focused on compliance with the provisions governing the gambling organisation and running (by 315 controls more compared to 2020). The authorities authorised to perform the customs and tax controls in the area laid down in the *Act on gambling* in 2021 were the heads of the customs and tax control offices.

The gambling sector alone is differentiated in terms of vulnerability to money laundering or terrorism financing potential. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of ML in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

In the gambling sector, online gambling was ranked among the 5 products and services most frequently mentioned both by the cooperating units and the obligated institutions in terms of threat of money laundering. According to the above, the main threat factor is not the specific games or forms of gambling, but the nature of online transactions. Practically or gambling products are available online. The threat may be also exaggerated by anonymisation of the transactions on the gambling market (in particular at the foreign operators') caused by using the Internet for transaction purposes. Some products existing on the online gambling market pose a particular risk, since they enable betting via several accounts and place a bet on practically any potential result, which reduces the risk of loss. In the event of the online poker (in particular at the foreign operators') there is also the potentially a particular risk of collusion.

billion in 2021. This means that the gray zone – in terms of turnover – accounted for 51.0% of the entire online casino and betting market in the last year. Thus, the State Treasury lost PLN 782 million from unpaid gaming tax in 2021. According to the EY expert estimations, in 2021 the value of turnover on the gray casino and betting market amounted to PLN 27.7 billion, which accounted for 51.0% of turnover on this market. This study provides also that 22% of the Polish online gamblers use foreign currencies to gamble in the illegal casino or at the illegal bookmaker's. More than 16% of gamblers use the VPN apps. These two solutions are the method to avoid the blockages of non-licensed gambling operators. Cryptocurrency payments become increasingly popular.

[67] Information on the implementation of the *Act on gambling* in 2021; Warsaw, 2022, https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/raporty/ access on 27.01.2023

As a matter of principle, online gambling should be based on payments from the bank accounts or payment accounts, on which the customer is already identified and verified by the obligated financial institutions providing these accounts to the customer. Nevertheless, in in the case of certain gambling platforms of the foreign operators, it is possible to use less identifiable payment methods, i.e. anonymous/pre-paid electronic money or even cryptocurrencies, if allowed. This applies in particular to the gambling platforms having no licences, which are not subject to customer due diligence and keeping the registers and reporting requirements. These platforms are not controlled by any supervisory authority. There are also the cases, where an online gambling platform is located in one EU Member State, while the electronic money issuer provides access to the funds in the other Member State. Sometimes, the gambling platforms are licensed in one state, but operated in the other state via an intermediary. Such situations trigger the jurisdictional conflict, which jurisdiction is competent to carry out the supervisory activities and from what perspective to investigate the compliance with the AML/CFT requirements.

The gambling market provides potentially wide opportunities of breaking the penal provisions. The Police forces, when describing the methods applied by the offenders with the use of the Internet, indicated the potential option to skip the Polish regulations and transfer the illegal gambling to cyberspace; in the area of online gambling affecting the money laundering potential, the Police forces identify the following several modi operandi:

- the rules and regulations of the online casinos not licensed in Poland allow for transfer of funds between the customers without using the casino account. In effect, the customers may potentially borrow the funds from unknown and non-verifiable sources. In this way, such casinos increase the threat of money laundering or terrorism financing, making it possible to use the funds from illegal activity in the transactions;
- vast majority of online casinos have implemented the provisions on deposit. This is the amount that needs to be paid to participate in the general transactions or the amount that needs to be paid to apply for a casino bonus. Many e-wallets accept cash as the deposits. The customers credit the e-wallet using the financial institution account, while confirmation issued by this institution will consider only the payment to e-wallet rather the transaction with the online casino;
- in the event of a poker game in the Internet, this game frequently takes place on the platforms shared by many casino operators. The platform itself plays the key role in pattern monitoring and value of game from the perspective of the potential money laundering activities, for example chip dumping. This strategy is based on that the gamers in collusion intentionally move in the way aiming at artificial control of the chip distribution (e.g. to one pre-defined gamer) to ensure benefits;
- when using online gambling, the offenders credit the relevant account linked with a gambling platform of a foreign operator. Then the funds are transferred back to the platform customer in the form of so called “win”, which enables hiding the identification data of the gambler, in particular in the case of foreign online casinos.

In the gambling sector, low threat and demonstrated low vulnerability to money laundering and terrorism financing of the gambling sector should be assigned to raffles. Taking into account the gambling market as a whole, the raffles are a niche and negligible in terms of turnover volume type of gambling. In contrary to the other types of gambling, raffles allow the participation of the minors. The specific features of raffles include in particular the dependence

of the result from a chance, the necessary specification of the terms and conditions of the game in the rules and regulations and offering by the organising entity of only in-kind prizes (winning money is impossible). Raffle is organised in accordance with the permit, which may be applied for by a natural person, legal person, or an organisational unit without legal personality. If the value of the pool does not exceed the value of basic amount, it is sufficient to notify the organisation of raffle to the competent Head of the Customs and Tax Control Office in at least 30 days prior to the scheduled event. If the raffle is organised by the public benefit organisation, the value of pool may amount up to 15 times the basic amount, subject to the limit of the total value of pool not exceeding the 30 times of the basic amount. The organiser of such raffle must, in 30 days upon its completion at the latest, submit the raffle report. The lottery tickets must be duly secured i.e. must be secured against manipulations and the organiser needs to enable their control. Also the persons organising the raffle must meet specific requirements, for example must have a clean criminal record. In addition, income from raffle must be entirely allocated to the implementation of the public benefit goals specified in the rules and regulations of the game, in particular charity. The basic amount for determination of the value of prizes in 2022 was PLN 5774.13. 15 times this amount is PLN 86,611.95, while 30 times is PLN 173,223.90. Apart from the potential manipulation with the nominal value of prizes, the raffles provide the theoretical option of transfer of the several hundred thousand values, however in practice, vast majority of raffles has much lower values of prizes. Since vast majority of raffles have been organised by the non-governmental organisations as a part of occasional events for a given community and the value of estimated amounts of prizes in these raffles is relatively low – the area of raffles may be specified as the area of low threat of money laundering and terrorism financing. In most cases, the prizes are small items of low value, usually handmade or acquired from local community. The average value of items transferred during raffle drawings is impossible, however their total value is not higher than the 15 times the basic amount. Their practical value, from the perspective of exposure to money laundering or terrorism financing is relatively negligible. In order to reflect the scale of trading for raffles, the total tax declared by the taxpayers amounted to PLN 13 thousand in 2019 and PLN 4 thousand in 2020. The year-to-year decrease by PLN 9 thousand i.e. by 67.1% was recorded. When comparing the tax in the area of raffles and the tax in the area of for example cash lotteries (PLN 225 million in 2019 and PLN 2019 million in 2020), the incidental share of raffle tax (practically negligible) in the total gaming tax is noticeable. This undoubtedly demonstrates the values of money traded in raffles, which are negligible for the gambling area as a whole.

According to the Supranational Risk Assessment (SNRA) there are no evidences that the terrorist groups used the online gambling platforms for the purposes of terrorism financing. It seems however that certain systemic gaps in the online gambling regulations create the potential for the possible future frauds by the terrorists and their supporters, who would be able to finance terrorism with the use of this sector. In its practice, the GIFI has received no information on the possibility to use the modus operandi involving the online gaming sector, including online gambling, in Poland for the purposes of terrorism financing. There is also no information that this sector acted as the area of operations of the Polish law enforcement authorities with a view to terrorism financing.

Averaged level of threat of the gambling sector – ML – 2.75 and FT – 1

Averaged level of vulnerability of the gambling sector – ML – 2.0 and FT – 2

Estimated level of probability for the sector – ML – 2.30 and FT – 1.60

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60%

(vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the gambling sector – 1.56	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the gambling sector – 2.38	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the gambling sector for the purposes of terrorism financing in Poland is at a low level.

CONCLUSION 2: The level of risk of using the gambling sector for the purposes of money laundering in Poland is at a medium level.

Mitigation of the identified risks:

In order to mitigate the probability of using the gambling sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The obligated institutions from the gambling sector should put particular attention to the cases of crediting the larger volumes of cash, in particular by the non-EU residents. Obtaining information on the source of origin of assets, for example by verification of the foreign currency declarations of the customers from the non-EU states would be reasonable.

The obligated institutions should put particular attention to the on-going analysis of the transactions made by the customers being the gambling undertakings and the customers earning profits from gambling. This applies in particular to the customers withdrawing profits from gambling from the foreign operators.

The gambling sector operators including these providing online services should deploy and develop the advanced IT tools and systems supporting the implementation of the objectives of anti-money laundering and counter-terrorism financing, in particular by streamlining and automation of processes linked with the on-going transaction analysis.

The gambling sector operators should enhance the activities related to the appropriate assessment of business relationships, in particular by obtaining relevant information on the customer, source of origin of assets and the purpose and intended nature of business relationships. The need to update the collected customer information should be also emphasized.

The gambling sector should undertake the actions raising the awareness of exposure to money laundering and terrorism financing offence, as well as increasing the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The obligated institutions from the gambling sector should put particular attention to the transfers of funds to the jurisdictions of higher risk of money laundering and terrorism financing (in particular withdrawals from the accounts of customers of the online service providers). The obligated institutions should place particular emphasis to determination of data on the source of origin of assets at the disposal of the customer as well as inability to obtain from the customer of the documents verifying the provided information on the source of origin of the assets.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of the source of origin of the customer's assets is of particular importance. The gambling sector operators should put particular attention to the customers from jurisdictions in the conflict zones, placing the bets with high amounts of money or gambling aggressively.

10. Area – non-profit organisations

Sector description – is contained in the chapter 2.2 – "Non-financial market" and in the sub-chapter 7.2.2 - "Vulnerability of the financial market".

Risk occurrence scenarios (i.e. possible risk occurrence examples) referred to the use of charitable activity by foundations and associations for money laundering purposes; and use of

the funds raised for charity purposes scheme for financing the terrorist organisations. The description of scenarios is presented below.

Money laundering

Table 47

Type of used services, financial products	Charitable activity
General risk description	Use of foundations and associations for money laundering purposes
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The criminals transfer through various straw men and shell companies the illicit proceeds to the foundations of associations controlled by them as donations. The funds are then transferred to the offenders or associated persons as the scholarships, allowances, loans for business activity, correspondingly to the statutes of these entities. 2. Establishment of a non-profit organisation for money transferring (as "remuneration") to the persons employed illegally at the territory of the Republic of Poland.
Level of vulnerability	3
Justification for the level of vulnerability	Establishing a foundation or association is hindered (meeting the specific obligations is required, among others preparing the statute, registration in the National Court Register, followed by the supervision by the public administration authorities). Hiding the identification data of the true donors and beneficiaries is easy, in particular when the foundation or association is controlled by the perpetrators. Transactions of international nature are possible. The foundations and associations with legal personality are the OIs only in the scope, in which they accept or make payments in cash of the value equal to or exceeding the equivalence of EUR 10 thousand, regardless of whether the payment is made as a single operation or several operations which seem interlinked. Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. They submit no or relatively little information on the suspicious transactions/activity to the GIFI. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	Use of the mechanism consisting in establishing the foundations and associations, through which the funds will be transferred to the selected beneficiaries, may be perceived in Poland as a relatively attractive method of money laundering. Dirty money – in many schemes – may be transferred to the legally operating foundations or associations, only to – in accordance with the statue of a given foundation/association – credit the specific beneficiaries or their companies with already legitimised funds. The donors may include the domestic or foreign entities, contact with which – in the case the investigation is needed – may be impossible. The freedom to dispose funds by each holder and no need to explain the decisions on donating a specific foundation affects the attractiveness of this *modus operandi*. Using this method requires from the entity legalising the proceeds of crime no highly specialist knowledge, wide-scale planning or unique skills. This method is sometimes accompanied by the advisory services provided by law offices or specialised tax firms. In some cases, false documentation may be used. CONCLUSION: Establishing the foundations and associations for the purposes of transferring funds from illegal sources poses a high threat of money laundering.

Terrorism financing

Table 48

Type of used services, financial products	Charitable activity
General risk description	Using the funds raised for charity purposes for financing the terrorist organisations
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Using the charity organisations (registered and unregistered) controlled by the terrorists to raise and transfer funds for the purposes of terrorist organisations. 2. Allocation of funds for terrorism financing through the persons operating under the non-profit organisation (NPO) – at the stage of fund raising i.e. before crediting the organisation account with these funds. 3. A supporter of a terrorist group, having access to the funds raised by a legal charity organisation as its employee, responsible for their accounting or supervision over this area, facilitates their transfer for the purposes of this terrorist group. 4. Personating by the terrorist group supporters as the legally operating charity organisations and raising funds under the fictitious titles to transfer them for the purposes of these groups. 5. In the charity organisation controlled by the terrorist group supporters, the funds raised for the purposes of humanitarian aid are blended with the funds collected for terrorist purposes in order to hide them and transfer more easily to these terrorist groups. 6. The funds raised for legal charity purposes – upon their transfer to the places of destination in the conflict zones or nearby – are taken over by the terrorist organisations for their purposes. 7. Collecting by the money transfer service providers of a “tax” for transfer of funds from these organisations to the area of destination. This “tax” is then transferred to a terrorist organisation operating at a given territory. 8. Transfer by the NPO of funds from the donors to a foreign NPO, which allocated the received funds for the purposes of terrorism financing.
Level of vulnerability	3
Justification for the level of vulnerability	Establishing a foundation or association is hindered (meeting the specific obligations is required, among others preparing the statute, registration in the National Court Register, followed by the supervision by the public administration authorities). Hiding the identification data of the true donors and beneficiaries is easy, in particular when the foundation or association is controlled by the perpetrators. Transactions of international nature are possible. The foundations and associations with legal personality are the OIs only in the scope, in which they accept or make payments in cash of the value equal to or exceeding the equivalence of EUR 10 thousand, regardless of whether the payment is made as a single operation or several operations which seem interlinked. Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. They submit no or relatively little information on the suspicious transactions/activity to the GIFI. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2

Justification for the level of threat	The charity organisations may be used by the terrorist groups for financing purposes in various ways. This may include direct transfer of a part of funds acquired by the NPO for the purposes of terrorist activity, or transfer of all funds acquired by the NPO, when such organisation only camouflages the terrorist activity. A charity organisation may be also actually involved in charity, however the aid is granted by the units of this organisation, which are controlled by the members associated with the terrorist groups. This leads to the situation, in which the aid beneficiaries believe that they receive support from a terrorist organisation. Such method brings significant propagandistic benefits. NPOs are used by the terrorist organisations, since – due to their charitable activity – they enjoy widespread social trust. The content distributed through NPOs significantly affect the attitudes of people, while the potential counteractions taken by the state authorities may face the allegations of persecution, racism, violating human rights. The use of this *modus operandi* is perceived from the a/m reasons as relatively attractive and safe. Logistical preparations of such operations require moderate skills. The GIFI has received little information on the opportunities of using this method to finance the terrorist activity. CONCLUSION: Using the charity organisations for the purposes of terrorism financing in Poland poses a medium threat of terrorism financing.

The Polish legislation, such as the EU legislation, has no legal definition of a non-profit organisation. The non-profit organisations are the social non-governmental organisations, which – in their operation – aim at supporting the private or public good without the focus on earning profits. Referring to the definition of non-governmental organisations provided for in Article 3(1) of the *Act on public benefit activities and volunteering,* these include primarily the foundations and associations classified as non-governmental organisations[68] of non-profit nature and as such governed by this Act, however having the option of applying for the public benefit organisation status or benefiting from public administration subsidies.

Recognition of non-profit activity as the area of the risk of frauds for the purposes of money laundering or terrorism financing is associated with the FATF recommendations. In its Recommendation no. 8 FATF indicated that the countries should take all efforts to ensure that the non-profit organisations (NPO) are not abused for money laundering or terrorism financing purposes. Pursuant to the FATF definition, NPO should mean a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"[69].

The foundation, in the wording as laid down in the *Act of 6 April 1984 on the foundations* is a legal form of a non-governmental organisation, in which the important element is the capital allocated to a specific purpose. The foundation may be established for socially or economically beneficial purposes compliant with the essential interests of the Republic of Poland, in particular such as: health protection, economic and scientific development, education and

[68] The non-governmental organisations are as follows:
1) other than the public finance sector units in the meaning of the *Act of 27 August 2009 on public finance* or the enterprises, research institutes, banks and commercial law companies being the state or self-governmental legal persons,
2) not operating for profit
– legal persons or organisational units without legal personality, granted with legal capacity under a separate act, including the foundations and associations, subject to section 4.

[69] Best practices - Combating the abuse of non-profit organisations (Recommendation 8), FATF, June 2015, https://www.fatf-gafi.org/fr/publications/Inclusionfinanciere/Meilleures-pratiques-abus-obnl.html

upbringing, culture and art., social aid and support, environmental protection and the protection of historical monuments. The association is a basic organisational and legal form implemented the constitutionally guaranteed and one of the most important civil rights – the right of freedom of association and joint actions. Pursuant to Article 2(1) of the *Act of 7 April 1989 – Law on Associations,* an association is a "voluntary, self-governing and permanent association of non-profit purposes".

The non-profit organisations have been operating in European in four basic models of activity. Firstly, there is the Scandinavian model with more than 200 non-governmental organisations per 10 thousand of inhabitants. The feature of the Scandinavian model of the sector operation[70], which has the greatest impact on such extensive „saturation" of these countries with the organisations, is a high level of participation in the associations (depending on the source, from 50% to even 90% of citizens are associated in an organisation). Secondly, there is the Rhenish model existing in Germany and Belgium (as well as for example in Austria). The difference between this and the Scandinavian model consists in the division of tasks between the state and the social service organisations. In the Scandinavian countries, it is the state that is responsible for the provision of such services (however it provides them in a highly decentralised manner), while in Germany or Belgium the public tasks in the area of social policy are performed by the non-governmental organisations (on the basis of contracting). The Anglo-Saxon model (operating for example in United Kingdom, United States or Canada) differs from the above ones. It differs from the Rhenish model among others with a distinct position of the organisation on the social service market. In Germany or Belgium, these organisations are preferred as the public task contractors, while in the Anglo-Saxon model they must compete for public funds (contracts) or private funds (in the form of payment for services) with the business. This leads to professionalization and marketisation of the organisations as well as large competition in the sector. There also the Mediterranean and Central and Eastern Europe models, where the principles of operation are more difficult to capture. They are subject to changes and modifications.

Vulnerability of the sector

Pursuant to the Act of 1 March 2018 on counteracting money laundering and financing of terrorism, the foundations and associations become the obligated institutions, if they have legal personality, were established under the *Act of 6 April 1984 on foundations* and under the *Act of 7 April 1989 – Law on Associations* respectively, as well as accept or make cash payments of the total value equal to or higher than EUR 10,000, regardless of whether such payment is made as a single operation or several operations, which seem to be interlinked. They will be also the obligated institutions, when they operate in the area of the games of chance in the meaning of the *Act on hazardous games,* for example charity raffles as well as when they conduct the activity in the field of keeping the accounts.

On the basis of data made available by the Klon/Jawor Association in the report „2021 Condition of the non-governmental situation – key facts" issued at the end of December 2021, Poland had 107 thousand associations /without the Voluntary Fire Brigades/ and 31 thousand of foundations registered, including only 70 thosuand of active associations and foundations. In the report on the implementation of the *Act of 1 March 2018 on counteracting money laundering and financing of terrorism* in 2021, the GIFI stated that according to information

[70] https://publicystyka.ngo.pl/ile-organizacji-jest-w-polsce-i-na-swiecie, access on 28.01.2023

obtained under Article 14(4) of the AML/CFT act from the starosts, voivodes and ministers, 18 obligated institutions were identified in total (as of 31 December 2021). Among the obligated institutions supervised by the a.m authorities, there were 9 associations and 9 foundations. Considering the fact that only one third of the entities obliged to provide information on the associations and foundation under Article 14(4) of the AML/CFT Act actually provided this information, it should be stated that the number of associations and foundations being the obligated institutions in Poland is low. In addition, on the basis of information submitted by 92% of starosts (they control the fulfilment by the obligated institutions – associations and foundations – of the obligations in the area of anti-money laundering and counter-terrorism financing) assessed their human and financial resources as sufficient to implement the tasks in the area of anti-money laundering and counter-terrorism financing, while 8% assessed their human and financial resources as insufficient. In vast majority of starosties, one or two trainings in the area of anti-money laundering and counter-terrorism financing were carried out in 2021.

The associations and foundations being the obligated institutions, should apply the customer due diligence measures listed in the Act of 1 March 2018 on counteracting money laundering and financing of terrorism. These measures cover primarily the activities related to the identification of customer and verification of its identity; identification of the beneficial owner and taking reasonable measures to verify its identity and determinate the ownership and control structure in the case of a customer being a legal person or organisational unit without legal personality. In addition, the associations and foundations being the obligated institutions should assess the business relationships of the contractor and (where appropriate) obtain information on their purpose and intended nature. They should also monitor the business relationships of their customers on the on-going basis. Vast majortiy of the associations and foundations in Poland are not the obligated institutions. This results among others from the fact that the average annual budget of the non-governmental organisation in Poland in 2020 amounted to PLN 26 thousand. In the revenue structure of the NGOs in 2020, the dominating range was between PLN 10 and 100 thousand, which covered 36% of the organisations. The budget of 23% of non-governmental organisations was between PLN 100 thousand and 1 million, while of 6% of non-governmental organisations in Poalnd was above PLN 1 million.

In its practice, the GIFI noted that among the analytical proceedings initiated by the GIFI in 2016-2018, the percentage share of the proceedings in which the entities with “association” or “foundation” in the name were registered, was relatively low (approx. 1.2 % of all analytical proceedings). wszystkich postępowań analitycznych). A similar percentage share was also recorded for the analytical proceedings, in which in 2016-2018 the notifications to the prosecutor’s offices were sent and in which the entities with “association” or “foundation” in the name were registered, compared to all analytical proceedings with notifications to the prosecutor’s offices with regard to the suspected money laundering (i.e. approx. 1.2%). There were only 6 proceedings, in which the entities with “association” or “foundation” in the name were registered, among the analytical proceedings initiated by the GIFI in 2019-2022.

The non-governmental oganisations must apply the transparency strandards. The organisations should notify of the activities and projects, in which they participate and which they organise. The obligation of transparency of activity covers information on from where the organisation receives the funds, how it operates internally and to whom it provides support. For example, if a non-governmental organisation opens an account in the bank, it reports it to the tax authority on a dedicated form. This obligation applies to each subsequent bank account. One-off

donations from a natural or legal person exceeding the amount of PLN 15,000 are submitted to the tax office on a dedicated form, and information on this fact are made publicly available. If the amount of all donations received from a single legal or natural person exceeds PLN 35,000, the non-governmental organisation notifies the tax office on a dedicated form, and information on this fact is made publicly available. The non-governmental organisation and its employees are obliged to provide settlements of various activities, finance, policies and other initiatives.

The non-governmental organisations accept various forms of financing. The general operating grants are allocated for covering the general current expenditure and supporting the organisation's mission, while project financing is allocated for the specifc project purposes. The non-governmental orgnisations may also receive the funds from grands. The associations and foundations may be also financed from the donations, usually from natural or legal persons; subsities; paid public benefit activity; business activity; public fundraising; donations in cash or in-kind; sponsoring; charity auctions. Regardless of the source, the funds donated by the donors are of the key importance for the existence of non-governmental organisations and allow their continuous operation.

A large part of the non-profit organisations is involved in humanitarian aid i.e. saving and protecting lives during the natural or man-made disasters, as well as providing the necessary aid and support to the people exposed to long-term crises. They provide aid during the military conflicts or handling its effects. Due to operation in such difficult socio-geogpraphic conditions, the non-profit organisations may be exposed to infiltration by the criminal or terrorist organisations, which may hide the beneficial owner of the donated or received funds and impede tracking of the financial flows. The non-profit organisations providing the services may be directly exposed in particular to terrorism financing due to the nature of these organisations, which cover financing to and from the conflict areas or to the neighbouring states.

In the case of the obligated institutions being the associations and foundations, there is however the supervision laid down in the *Act of 6 April 1984 on the foundations* and of the *Act of 7 April 1989 – Law on Associations,* performed for foundations by the ministers and starosts and for the associations by the voivodes and starosts. These regulations however provide for no powers for these authorities in the area of verification of the statements or the accounting of financial documents of the associations and foundations to identify, which of them are the obligated institutions. Performing a relevant review and proposing the potential amendments to legal regulations on the associations and foundations enabling the competent authorities to perform the effective supervisory activities were provided for in the *anti-money laundering and counter-terrorism financing strategy*[71].

When assessing the level of vulnerability for the anti-money laundering and counter-terrorism financing system in the area of non-profit organisations, one should take into account the potential infiltration or takeover of these organisations by the organised crime groups, or alternatively takeover of the key positions in these organisations in order to manage them. This is of importance primarily from the perspective of the opportunities of terrorism financing by these organisations.

[71] RESOLUTION NO. 50 OF THE COUNCIL OF MINISTERS of 19 April 2021 on the adoption of the strategy for counteracting money laundering and financing of terrorism.

The sector of the non-profit organisations itself is differentiated in terms of vulnerability to money laundering or terrorism financing options. This results from the diversified area of activities, covering among others sport, tourism, recreation and hobbies, education or culture and art. Significant differentiation in the forms of acquisition by the associations and foundations of funds enabling effective operation of these organisations also plays an important role in vulnerability. The funds may be obtained in a highly anonymised form e.g. by cash donations or social fundraising.

Although these entities have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilment are still revealed. They submit no or relatively little information on the suspicious transactions/activity to the GIFI.

The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

In terms of assessment of risk of money laundering and financing of terrorism in the non-profit organisations sector, the particular threat is posed by the situations, where the operation of the associations or foundations concerned have personal links and contacts with the persons and entities from the states of high risk of money laundering and terrorism financing. It is similar in the case of operation of the foreign foundations or associations having their seat abroad and establishing the representative offices at the territory of the Republic of Poland. In such situation, there is a serious threat that a foreign terrorist group may pose as the legal entities, for example foundations and associations, and acquire funds for the terrorist purposes. There can be also the non-profit organisations associated with the persons representing the extremist movements. The non-profit organisations linked personally or ideologically with the persons representing the extremist movements (e.g. extremely Islamist, right-wing, left-wing) may support the entities or persons by among others organisations of fund raising campaigns, financing the paramilitary trainings or propagandistic events and materials.

Another situation linked with ML and FT threat is providing humanitarian aid at the areas of high risk of terrorism financing. In such case, the foundations or associations providing humanitarian aid at the territories of such high risk being the areas of military conflicts or active operation of non-state military groups or terrorists – are exposed to infiltration or even takeover of the organisation by the terrorist organisations. It is also possible that such organisation will serve as a cover for terrorism financing.

The ML and FT threat is also posed by representing the foundation or association by the politically exposed persons (PEPs). Also the personal links of the members of management board of the non-profit organisations with the business entities being the contractors of the foundation or association poses the ML and FT threat. Conducting the activity under the address of so called virtual office is also a warning signal.

Threat is also posed, when a foundation or association starts a business activity in contrary to the statute.

A vast majority of non-profit organisations benefits from several financing sources (58% of them has no more than 3 financing sources). However, such numerous financing sources enable hiding the transfer of illicit proceeds to the non-profit organisations for the purposes of their laundering. For example, money obtained from crime, paid as donations by straw men or non-existing natural or legal persons, may be further – legally – transferred to specific persons or business entities, allegedly in compliance with the purposes specified in the statute of the organisation.

The source of threats in the non-profit organisations sector can be using the methods of collecting funds, which facilitate hiding their source of origin and the identity of actual donors (for example a part of public fundraising campaigns, charity auctions). Using the new technological tools facilitating hiding the source of origin of funds, such as "crowdfunding" (crowdfunding) or "blockchain" (transactions in virtual currencies) may also be a source of threat.

In each case, absence of publicly available information on the website about the foundation or association, in particular on the scope of activity, exemplary initiatives or the way of using the funds – according to the statute, should raise concerns in each time. This applies also to lack of information on the ultimate use of the funds. A short period of the foundation or association operation combined with unusually high turnover should also be treated as a red flag.

The potential threat is also posed by obtaining negative information on the operation of the foundation or association, which may for example indicate their use to commit an offence. A similar situation is receiving information on, for example, suspending the management board of the foundation and appointing a receiver or suspending the management board of the association in its activities and appointing a representative to handle current activities of the association.

The Europol TESAT 2022 report contains information that several Western Balkan countries confirmed the trend, which has been observed in the previous years, that some extremist groups present themselves and non-governmental humanitarian organisations. Acting as such aid organisations, they collect donations, which are then transferred to the supporters of the extremist Islamist ideologies. In some cases, these groups have established contacts with the communities of Western Balkan migrants in the EU countries. This report presents also the cases of terrorist groups using the non-profit organisations to raise money under the cover of charity collections. In Spain, three suspects using such scheme were arrested for terrorism financing. Money was collected by a religious organisation under the pretext of humanitarian aid for the Syrian orphans, however in reality were transferred to finance the Al.-Qaeda fighters in Syria via a non-profit organisation.

In addition it was noticed that some foundations openly collect funds for the Foreign Terrorist Fighters and their families in the conflict zones and prison camps in Syria.

On the FATF forum, several countries pointed out at the opportunities to use the non-profit organisations sector for terrorism financing purposes. The Republic of South Africa informed that the non-profit organisations have been used to generate funds for terrorist purposes. These funds are then transferred to the Islamic State and associated entities. United Kingdom recorded

the cases of fund raising by the Islamic State by the agency of the shell companies, charity organisations and e-platforms. The Russian Federation informed on the cases of using the charity and non-governmental organisations for the purposes of acquiring funds for terrorist activity conducted under the pretext of implementation of human rights, humanitarian and charity programmes in some countries. The received funds are allocated to promote the terrorist ideology and encourage the recruits to join the armed gangs in the Middle East, Europe and the Commonwealth of Independent States countries. The nature of operation of these organisations is usually religious. At the same time, the true purpose of collected funds is in many cases not revealed to the management of these organisations. The organisations' staff include the extremists, who use the charity projects to find the new fighters and establish the units in various countries around the world. These activities are carried out at a high conspiracy level.

Due to the nature of their operation, the non-profit organisations are diversified in terms of the level of risk of money laundering and terrorism financing. Large non-profit organisations of a formalised structure involved in the intermediation in transferring funds for socially useful purposes may be infiltrated by the criminal or terrorist organisations. These organisations may hide the beneficial owner and impede tracking the financial flow, however their operations are subject to customer due diligence in the area of money laundering and terrorism financing. Such threat of money laundering and terrorism financing may be however reduced by the way of receiving the funds and supervision over their distribution by the donor. For example, a large part of the non-profit organisations receives funds for financing the humanitarian aid from the European Union funds or from the member states. These funds are subject to the strict contractual framework and high reporting standards with a view to their use as intended. In addition, the EU and member states funds for the humanitarian aid are transferred through the non-governmental organisations selected on the basis of the pre-defined legal, financial and operational criteria.

Non-profit organisations providing direct charity services (organising the in-kind and financial support with the use of their members) may be exposed to money laundering and terrorism financing to a greater extent due to inherent, less transparent nature of their activity. This activity may cover direct financing to and from the conflict areas or from and to the states neighbouring the states described as the higher risk states.

Higher threat of money laundering and terrorism financing is also affected by the methods of financing of the non-profit organisations. The level of threat depends on the sources of financing of these organisations, in particular in the case of unknown sources of donations, cash, international sources or funds from high-risk countries. Higher threat of money laundering and terrorism financing depends also from the method of distribution of funds transferred for charity purposes, or using the informal channels to transfer the funds abroad. In addition, the level of threat of money laundering and terrorism financing is impacted by the type of operation of a non-profit organisation, its professionalization, and the type and nature of beneficiaries of aid provided by the non-profit organisations. The threat increases when the aid beneficiaries are the unknown or hardly known entities, located in particular in the high-risk countries.

In objective terms, the threat of money laundering and terrorism financing increases, when the non-profit organisations operate in the areas of geographically high risk of money laundering and terrorism financing. These areas include the conflict zones covered by military actions, in which the non-state military groups or fighters described as terrorist are present. The activity

of non-profit organisations in the states directly neighbouring such conflict zones also contributes to increasing the threat of money laundering and terrorism financing.

Although in most cases the term of non-governmental organisation or non-profit organisation is used when referring to the foundations and associations, such organisations include also the sports clubs and student sports clubs, organisations operating under the separate provisions, such as Polish Red Cross, Voluntary Fire Brigades Association of the Republic of Poland, Allotments Owners Association, hunting associations, social committees (e.g. social road construction or water supply system construction associations), territorial self-government associations, social cooperatives, political parties, labour unions, professional self-governments, federations and confederations of the employers, economic chambers, chambers of craft, church organisations, associations of farmers, machinery rings and farmer wives' associations, groups as the neighbours' clubs or support groups and self-help groups. Since financing of such organisations is associated with a specific need and for the purposes related to a specific project, stipulated by law[72], the risk of money laundering and terrorism financing by such organisations is low.

In Poland, the National Prosecutor's Office supervising the investigations in terrorist cases, have not analysed the involvement of non-governmental organisations yet, including in particular of the foundations and associations, in the crime of terrorism financing. Only the investigation of the Podlaski Branch Division of the Department of Organised Crime and Corruption of the National Prosecutor's Office in Bialystok, in which four citizens of the Russian Federation were charged of terrorism financing, revealed that the transfer of in-kind support in the form of paramilitary products to the persons involved in terrorist activity was made through the employees of the "Ocalenie" Foundation providing humanitarian aid to the Chechen refugees. The Foundation itself was not involved in terrorism financing.

Averaged level of threat of the non-profit organisations sector – ML – 3.0 and FT – 2.0

Averaged level of vulnerability of the non-profit organisations sector – ML – 3.0 and FT – 3.0

Estimated level of probability for the sector – ML – 3.00 and FT – 2.60

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the non-profit organisations sector– 2.16

[72] for example, the voluntary fire brigades are the fire protection units being in formal and legal terms the associations in the meaning of the *Act of 7 April 1989 – Law on Associations*, however being at the same time the uniformed units, equipped in specialist equipment and serving to fight fires, natural disasters or other local threats, including in the area of specialist rescue services provided by the fire-fighting units.

1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the non-profit organisations sector – 2.80	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the non-profit organisations sector for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the non-profit organisations sector for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the non-profit organisations sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The foundations and associations with legal personality are the obligated institutions only in the scope, in which they accept or make payments in cash of the value equal to or exceeding the equivalence of EUR 10 thousand, regardless of whether the payment is made as a single or several operations, which seem interlinked. The mitigating factor of risk related to the operation of non-profit organisations are the control powers related to the anti-money laundering and counter-terrorism financing obligations, however it is necessary to improve the procedures to ensure efficient exchange of information on the non-profit organisations, which fulfil a statutory prerequisite for recognition as an obligated institution in a given period.

The non-profit organisations sector should undertake the actions increasing the awareness of exposure to the crime of money laundering and terrorism financing, as well as increasing the level of organisations' staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

The obligated institutions from the non-profit organisations sector should put particular attention to the transfers of funds to the beneficiaries of the organisations from the jurisdictions of higher risk of money laundering and terrorism financing. The obligated institutions from the non-profit organisations sector should put particular attention to obtaining information on the purpose and intended nature of relationships linking the non-profit organisation with the beneficiary of funds collected by such organisation. A significant threat in the area of non-profit organisations is the possibility of infiltration or takeover of such organisations by the organised crime groups, or alternatively a takeover of the key positions in these organisations in order to manage them. The obligated institutions should draw their attention to updating information on the customers from the area of non-profit organisations in order to capture any change of operation of the non-profit organisations, with regard to the potential takeover of the organisation management by the persons intending to use such organisation for money laundering or terrorism financing purposes.

Due to the absence of publicly available information on the foundation or association in the Internet, in particular pertaining to the scope of activity, exemplary initiatives, or the ways to use funds specified in the statute, the obligated institutions establishing the relationships with an entity from the non-profit organisations sector should put particular attention to obtaining relevant and up-to-date information on the customer. The factors, which may indicate the attempt of using the non-profit organisation for criminal activity, should include in particular:

- starting a business activity in contrary to the statute by the foundation or association;
- personal links of the members of the management board of the non-profit organisations with the business entities being the contractors of the foundation or association;
- conducting a business activity at the address of so called virtual office;
- short period of operation of the foundation or association combined with unusually high turnover.

11. Crowdfunding

Sector description – is contained in sub-chapter 7.2.2 – "Vulnerability of the non-financial market".

Risk occurrence scenarios cover the potential of using a crowdfunding platform for the purposes of financing the illegal activity.

Money laundering

Table 49

Type of used services, financial products	Crowdfunding
General risk description	Organisation of crowdfunding actions to legitimise the available funds or transferred funds
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Organisation of crowdfunding actions, for example for starting a legal business activity, via a crowdfunding platform. The proceeds of crime are transferred by the straw men or fictitious natural persons in relatively low amounts. 2. Using the crowdfunding platforms to collect funds from unauthorised use of payment cards and their depositing/transferring onto subsequent bank accounts.
Level of vulnerability	4
Justification for the level of vulnerability	Launching a crowdfunding action is relatively easy, for example via social media. Hiding the identification data of donors and beneficiaries is easy. It is possible to make transactions of international nature.

	In theory, any can run a crowdfunding action. The entities running such actions are not the OIs. However, in the case of economic undertakings, the new provisions of the *Act on crowdfunding* have been in force since November 2021. In such case, the new obligation of holding a licence by the crowdfunding platforms and their on-going supervision by the Polish Financial Supervision Authority shall apply. Also the limit value of the amount obtainable by this form of financing has increased – from EUR 1 million to 5 million. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on such actions to a limited extent. It is probable that the case of money laundering in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation does not correspond to the scope of the analysed risk.
Level of threat	2
Justification for the level of threat	Crowdfunding is an alternative source of financing. It is the form of financing of various types of projects by a community, which is or will be organised around these projects. Money laundering, in the case of e.g. organised crime groups, is a type of undertaking and in this situation it is financed by a high number of small, one-off payments made by the persons, who participate in the money laundering process. The purpose of funds collection is usually not presented directly. Crowdfunding is inexpensive and as a *modus operandi* may be perceived by the perpetrators as relatively attractive and commonly accessible method of money laundering, yet bearing a significant risk. Usually the crowdfunding action lasts for a certain period of time, since it is relatively easy to target and additionally may end in a failure, which in effect makes this method relatively unattractive. Organising of a crowdfunding action may involve certain costs (crowdfunding platform intermediation is related to a commission of – in some cases – reaching even several percents, usually from the collected fund). In addition, it requires adequate planning and knowledge as well as the time for running thereof. The GIFI received very little information on the opportunities to use this method for money laundering purposes. CONCLUSION: Use of the crowdfunding mechanism poses a medium threat of money laundering.

Terrorism financing

Table 50

Type of used services, financial products	Crowdfunding
General risk description	Acquisition of the donors of funds for the purposes of terrorist organisations using the modern communications network
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Organising the actions via a crowdfunding platform to collect funds for the purposes of activity of terrorist nature. The actual purpose of fund raising will not directly indicate the intended use of the collected funds for terrorism financing. 2. The supporters of terrorist organisation appeal for the funds via social media. The donors transfer the donations in cash or virtual currencies to the initiators of the action, or purchase the international pre-paid cards and provide their numbers to the initiators. 3. Funds collection based on pre-sales for example of a book – in this model the funds are collected for the purposes of publishing a significant work literature or implementation of the individual stages of its creation. The donors are aware that the actual recipient of funds is a terrorist organisation.
Level of vulnerability	4

Justification for the level of vulnerability	Launching a crowdfunding action is relatively easy, for example via social media. Hiding the identification data of donors and beneficiaries is easy. It is possible to make transactions of international nature. In theory, any can run a crowdfunding action. The entities running such actions are not the OIs. However, in the case of economic undertakings, the new provisions of the *Act on crowdfunding* have been in force since November 2021. In such case, the new obligation of holding a licence by the crowdfunding platforms and their on-going supervision by the Polish Financial Supervision Authority shall apply. Also the limit value of the amount obtainable by this form of financing has increased – from EUR 1 million to 5 million. The public administration authorities have basic knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on such actions to a limited extent. It is probable that the case of FT in the scope of the analysed scenarios will not be detected. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation does not correspond to the scope of the analysed risk.
Level of threat	2
Justification for the level of threat	Crowdfunding is an alterative souce of financing, also of terrorist activity. It is the form of financing of various types of projects by a community, which is or will be organised around these projects. Terrorist activity, as a kind of undertaking, is in such case by a high number of small, one-off payments made by the persons interested in supporting the terrorist activity. The purpose of funds collection is usually not presented directly. Crowdfunding is inexpensive and as a *modus operandi* may be perceived by the perpetrators as relatively attractive and commonly accessible method of terrorism financing, yet bearing a significant risk. Usually the crowdfunding action lasts for a certain period of time, since it is relatively easy to target and additionally may end in a failure, which in effect makes this method relatively unattractive. The GIFI received very little information on the opportunities to use this method for the purposes of terrorist activity financing. CONCLUSION: Use of the crowdfunding mechanism poses a medium threat of terrorism financing.

The possibility to use this form of financing for the purposes of supporting the terrorist activity poses a particularly significant threat. The extremist organisations can easily use all types of collections for charity purposes, since they conduct a political activity and refer to the feelings of their supporters, who identify with the postulates of a given organisation. The funds may be collected for falsely described purposes, the true meaning of which are known only to the insiders, or may be collected for a purpose catchy for a specific community, and then used in any manner whatsoever. The object of support may include assistance to real persons for examples injured during the fights, who are actually the injured terrorist fighters. Such false purpose may be also a collection for a project, which is actually a form of building the terrorist organisation infrastructure. The actual use of the funds is supervised by the fighters. Propagating the collection among the supporters is also easy.

The use of a crowdfunding platform is less probable in the case of laundering of the proceeds of crime. Despite the above, a scenario, in which a crime group launches a false collection to legalise the illicit proceeds, is probable. Such scenario requires an organisation of a group of entities with reliable data and transferring them in the form simulating fair transactions. The funds legalised in such manner may be later used by the group to finance its activity or to distribute the profit to its members. Withdrawal of cash from the collection-dedicated account

may be made to the legally existing entities or to finance a legal project controlled by the offenders. This method of financing may be also used by the persons acting as the intermediaries or providing the money laundering services to the other entities.

Vulnerability

On 29 July 2022 the provisions of the *Act of 7 July 2022 on crowdfunding and assistance to the borrowers* entered into force. This Act implemented the Regulation EU 2020/1503 of the European Parliament and of the Council implementing the systemic regulations at the EU level to the Polish legal regime. The Act governs the internal organisation and operation of platforms. According to the Act, the consents for providing the equity crowdfunding services are granted by the PFSA. According to the above, the Commission holds the powers to supervise and control the operation of a given entity in this area. The limit value of the amount collected without presenting the issuing prospectus is set as the equivalence of EUR 5,000,000, subject to the use of platform registered through the PFSA[73]. The collections enable different forms of the legal tenders. The PFSA warns about the threats stemming from making investments in this form[74].

The crowdfunding platforms operate in virtual space. Therefore, a large part of them is registered outside the country. This reduces the possibility of full control over the operation of these service providers and the of the collection process itself.

Using the crowdfunding platform requires adequate planning and preparation. It is necessary to present the object of collection in a relevant manner, making it sufficiently reliable to not to raise any suspicions. The other requirement is the existence of a relevant group of donors making payments or simulating their existence. The collection process requires a high number of small payments. Despite these difficulties, a sufficiently determined crime or terrorist group is able to organise such collection.

Threats in the sector

A vast majority of payments on the crowdfunding platforms are small amounts, which raise no suspicions of the control authorities. A success of collection depends in this case from the existence of a relevant group of supporters, who can be mobilised to provide support by referring to religious or political beliefs. In addition, maintaining anonymity of the donors, who in most cases benefit from the wide spectrum of the support channels, from electronic payments, transfers via telecommunications services, to specific solutions such as donation machines is easy[75].

Running a collection for criminal purposes is particularly easy to the extremist organisations referring to the emotions and ethical attitudes of their supporters. In such circumstances, it is easier to mobilise the group of actually existing and therefore raising no suspicions persons to support the purposes of the organisation. At the same time, due to knowledge about the community addressed by a given organisation with its message, each started collection may be adequately profiled. If there are already any existing communication channels with the supporters, information on starting of the collection of funds may be disseminated much faster. At the same time, when arranging a group of actually existing persons, an advantage is a

[73]*Act of 7 July 2022 on the crowdfunding for the economic undertakings and assistance to the borrowers*,
[74]https://www.knf.gov.pl/dla_rynku/crowdfunding/inwestorzy, access on: 27.12.2022,
[75]How Card Payment Machines Can Help Charities (paymentplus.ie), access on: 27.12.2022,

diversity of methods used by the supporters, who may transfer the funds using various available means, which additionally impedes the identification of the sources of origin of transferred funds.

Collecting funds is more easier in the communities with the well-established culture of charity support. Such traditions as the Muslim zakat increase the resources of funds which may be transferred within crowdfunding. The potential donors may think that donating a specific persons satisfies their ethical and moral needs. This increases the number of the potential donors, ranging outside the group of supporters of the extremist ideas and covering the persons of moderate views, who may support a given purpose from ethical reasons, being unaware that they actually support a terrorist group. It can be assumed that in reality most of the collected funds may be donated by the persons not interested in supporting the fighting operations.

There has been information in media on collecting the funds for humanitarian purposes, which was actually transferred to support the operation of terrorist groups. The case revealed in Germany in 2022 referred to the funds collected by means of crowdfunding as a support for the families of fighters interned in the al-Hol camp in Syria. It was revealed that a part of funds were used to take some interned persons away and deliver them to the training camps of ISIS and other terrorist organisations[76]. Such events clearly demonstrate that supporting even the most ethically justified purposes may lead to financing of the extremist activity, since the donors are unable to verify how the collected funds are distributed. The organiser of a crowdfunding action is usually not required to present a detailed settlement, and the way of their actual use is usually easy to hide.

Due to the mechanism of action, the use of crowdfunding methods for the purposes of money laundering is of a different nature. In such case, it is necessary to organise a relevant number of reliable entities, who would be used to transfer the funds, and making payments by the agency thereof. There are no existing social resources that could be easily used to launder money, and the activity conducted in such conditions cannot be based on a wide group of actually existing persons, who would need to act with awareness to a certain extent. The offenders, acting cynically and deliberately, cannot base their activities on involvement due to ethical and moral reasons.

In most cases, crowdfunding is used as the mechanism of a predicate offence[77]. The donors frequently fail to verify the actual purpose of a collection, whether the intentions of the organiser are true or whether the persons (entities) in need actually exist. Passing off as the actually existing persons using the true documents and data is also possible[78]. If a crowdfunding portal has the internal collection verification system deployed, the controls cover only the process of funds collecting in the system. The portal acts as an intermediary between the donors and a beneficiary. The funds ultimately transferred onto the account of the collection organiser become its property and can be used for any purpose whatsoever.

Crowdfunding assumes supporting of a given project by a number of small entities, donating the collection with small amounts. The collection process performed via a crowdfunding platform can be effective with regard to the proceeds of crime with are not donated in large amounts. It is a convenient method for laundering the proceeds from electronic crimes, since in

[76]Crowdfunding the 'Islamic State' group – DW – 09/10/2022, access on: 27.12.2022,
[77]Bezpieczeństwo w firmie Najpopularniejsze oszustwa na (politykabezpieczenstwa.pl); access on: 09.03.2023,
[78]Żył z fałszywych zbiórek. Policja zatrzymała oszusta - Money.pl; access on: 09.03.2023

such case the entire money transferring process takes place in cyberspace. The advantage for the perpetrators is the fact that the transfer onto the account is sent from the crowdfunding platform i.e. the entity having in most cases a recognisable brand and being beyond any suspicion.

Crowdfunding is a relatively new financing tool and therefore a vast majority of operations of the crowdfunding platforms remains non-regulated. This applies in particular to financing of projects of philanthropic or aid-related nature. The description of threats related to the market points out at absence of clear and transparent AML/CFT procedures, even at the largest service providers'[79]. Unquestionably, absence of clear and transparent regulations and significant flexibility of the activity makes crowdfunding an attractive method of operation for a certain type of offenders and extremist groups. This is encouraged by a significant development of this sector in recent years, which has increased both the number of market operators and of the available funds[80].

Averaged level of threat of the crowdfunding sector – ML – 2.0 and FT – 2.0

Averaged level of vulnerability of the crowdfunding sector – ML – 4.0 and FT – 4.0

Estimated level of probability for the sector – ML – 3.20 and FT – 3.20

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the crowdfunding sector – 2.52	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the crowdfunding sector – 2.92	
1 – 1.5	Low
1.6 – 2.5	Medium

[79]Crowdfunding: A Criminal's Hiding Place? (linkedin.com), access on: 28.12.2022,
[80]Crowdfunding: Fraud and Money Laundering Risks - Sanction Scanner, access on: 28.12.2022,

2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the crowdfunding sector for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the crowdfunding sector for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the crowdfunding sector for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The obligated institutions involved also in crowdfunding as well as the obligated institutions, whose customers are the entities involved in crowdfunding, should put particular attention to the transfers of funds from or to the jurisdictions of higher risk of money laundering and terrorism financing.

The obligated institutions involved also in crowdfunding should put particular focus on obtaining information on the purpose and intended nature of the relationships between the customer and the beneficiary of funds collected by means of crowdfunding. The obligated institutions, whose customers are the entities involved in crowdfunding, should put particular focus on obtaining information from the customer on the purpose and intended nature of the relationships between the customer and the beneficiary of funds collected by means of crowdfunding.

The obligated institutions involved also in crowdfunding as well as the obligated institutions, whose customers are the entities involved in crowdfunding, should put attention to the transfers of funds onto the accounts not linked with the beneficiary of the collection, the transfers of funds to third countries, or to the cases of making a high number of donations onto the account

of a given collection in a short period of time, and also on the payments of an unusually high value, in particular from the foreign jurisdictions.

The obligated institutions involved also in crowdfunding as well as the obligated institutions, whose customers are the entities involved in crowdfunding, should monitor the business relationships on the on-going basis and, in justified cases, request the customer to provide information and documents on the payments made for the purposes of a given collection or beneficiaries of the organised collections. Open-source information (in particular in the Internet) on the intended purpose of a collection or containing the description of the collection beneficiary may be untrue. Misleading information in this scope may derive from the organiser of the collection or indirectly from the person or entity, for the benefit of whom/which the collection is organised. With regard to the above, the obligated institutions involved also in crowdfunding and the obligated institutions establishing the relationships with the crowdfunding sector entity, should put particular attention to obtaining relevant and up-to-date information on the customer, source of origin of assets, and in the course of business relationships also on the transactions for the benefit of the customer (payments made to a given entity).

12. Trade in high-value goods

Sector description – is contained in the sub-chapter 2.2 – "Non-financial market" and in the sub-chapter 7.2.2 – "Vulnerability of the non-financial market".

Risk occurrence scenarios cover the opportunities of acquire funds for financing the illegal activity from trade in high-value goods i.e. gold, precious stones, antiques, works of art, etc. They may also assume the use of such goods for allocation of the proceeds of crime. This circumstance refers primarily to the purchase of luxurious goods, antiques, works of art and goods serving as the allocation of capital, for example investment metals, precious stones. Goods can be purchased both for cash and other legal tenders or under counter-trade. The scenario covers also placing the goods obtained from theft or fencing on the market. In such case, they become a source of proceeds of an offender or a crime group.

With a view to terrorism financing, the scenario assumes the opportunities of importing the high-value goods to the country with the intention of their sale or transit. This may refer to the goods of culture stolen from the owners, acquired illegally or brought out of property of the other state, precious metals and stones acquired at the areas of warfare, etc.

Money laundering

Table 51

Type of used services, financial products	Precious metals and stones
General risk description	Investing the illicit proceeds in purchase of precious metals and stones
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The offenders purchase gold bars, gold coins, diamonds and other precious stones with the intention of their cross-border transportation (by courier or postal parcels and cargo shipments) and sale in the countries of less restrictive control of financial trading. Money from sale are then invested in legal undertakings or entered into the banking system. 2. The offenders purchase gold bars, gold coins, diamonds and other precious stones in the other countries for transferred illegal proceeds. The purchased goods are then sold legally in Poland or third countries on the basis of false invoices and certificates of origin. 3. The offenders purchase gold and silver jewellery and re-sale these items to the third-country companies involved in, for example, precious metals processing.
Level of vulnerability	3

Justification for the level of vulnerability	Although purchase and sale of relatively small amounts of such type of goods makes no greater difficulties (e.g. in the jewellery stores), it is just the opposite in the case of their large/wholesale purchase/sale. However, it is easy to avoid identification, in particular when purchasing/selling the goods of the value below the equivalence of EU 15 thousand. It is possible to buy/sell via Internet, and therefore make transactions of international nature (for example when purchasing stones or metals from a foreign entity). At present, the entities operating in the area of trade in precious or semi-precious metals or stones are not the OIs, provided that they do not accept or make payments for the goods in cash of the value equal to or exceeding the equivalence of EUR 10 thousand, regardless of whether the transaction is made as a single or several operations which seem interlinked, or provided that they do not conduct a currency exchange activity in the field of purchase and sale of FX gold and platinum. Poland enables purchase of gold in the form of bars and gold coins – so called bullion coins (without any numismatic value). Apart from that, the bullion coins are treated as a legal tender, which enables their transportation between the countries. In addition, import, processing and trade in diamonds is not a legally regulated activity, which means that it requires neither permit nor licence nor any other decision of a public administration authority. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	Using the mechanism of investing the illicit proceeds in the purchase of precious metals and stones is one of the most common methods of money laundering. Due to the stable value of metals and stones, easiness of transportation (even abroad) and relatively low volume making them easy to hid, this method is relatively frequently used. It is a commonly available method, its application is relatively inexpensive and is perceived by the perpetrators as rather attractive. Using the mechanism of investing the illicit proceeds in the purchase of precious metals and stones requires neither highly specialist knowledge nor specialist skills. The method is frequently used by organised crime, sometimes is associated with corruption, since in some cases requires preparation of false certificates or other documentation. The GIFI has received information on using this method for money laundering purposes. CONCLUSION: Using the mechanism of investing the illicit proceeds in the purchase of precious metals and stones poses a high risk of money laundering.

Table 52

Type of used services, financial products	Antiques and works of art
General risk description	Investing the illicit proceeds in purchase of antiques and works of art
Risk occurrence scenario (i.e. possible risk occurrence example)	1. The offenders purchase for illegal proceeds the antiques and works of art., which they keep as a kind of investment or transport abroad with the intention of sale. 2. Using so called NFTs[81] i.e. non-fungible tokens by the offenders (for example virtual works of art) for the purposes of entering the illicit proceeds

[81] a unique digital data unit based on the *blockchain* architecture, which can be traded between the protocol users, representing a wide range of tangible objects, i.e. among others the virtual works of art.

	onto the market, for example an organised crime group creates NFT for the purposes of its re-sale to the persons, which are also associated with this group. The transaction is made *on-line*.
Level of vulnerability	3
Justification for the level of vulnerability	Purchase/sale of antiques or works of art is relatively easy. There are many companies trading in this type of goods under the *Act of 6 March 2018 – Business Operators' Law* (auction houses, antique shops). It is possible to purchase/sale via Internet, and therefore make transactions of international nature. An important instrument, which has extended the spectrum of purchasing/selling the works of art on the market, including the international market, are the NFTs. Currently, functioning of so called *non-fungible tokens* is not regulated (the EU authorities pursue to adapt the legal regulations to this blockchain technology-based instruments). A subjective value of NFTs and lack of control over this instrument creates room for abuses in this field. At present, the operators trading or intermediating in trade in the works of art, collectors' items and antiques as well as operators providing the services of storage of works of art., collectors' items and antiques, if such activity is performed with the use of so called free port, for transactions of the value equal to or exceeding the equivalence of EUR 10,000, regardless of whether the transaction is made as a single or several operations which seem to be interlinked – are the obligated institutions in the meaning of the AML/CFT provisions. The provisions on business activity involved in trading in the works of art. and additional regulations (among others application of the AML directive and the need of keeping the record of historical objects accepted or offered for sale) impose strict obligations on the Polish market sellers, resulting in a precise identification of all parties to the transaction and transparency of the entire sale process, including the identification of the source of origin of the item. The existing and one of the most restrictive provisions on export and import of antiques compared to the European and global legislation provide the legally operating business entities have a full record of items imported and exported from the country. The activity consisting in trading or intermediation in trade in the works of arts, collectors' items and antiques acquired and smuggled from the areas of warfare in Ukraine remains however a great unknown. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2
Justification for the level of threat	Using the mechanism of investing the illicit proceeds in the purchase of precious metals and stones is one of the money laundering method. It is a long-term and profitable method, yet bearing some disadvantages. The key advantage of the works of art is a continuous increase in the value. Losing on such investment is quite difficult due to regularly growing demand and limited supply. The disadvantage is low liquidity. There is a very little number of high-value objects in trading on the market. Investing in purchase of antiques and works of art requires much patience and the profit depends on the trends. Investing requires the consulting services, need to prepare a valuation, and authenticity of the items may be problematic. Using the mechanism of investing the illicit proceeds in the purchase of precious metals and stones is perceived as rather unattractive method of money laundering. The GIFI has received little information on using this method for money laundering purposes. CONCLUSION: Using the mechanism of investing the illicit proceeds in the purchase of precious metals and stones is poses a low threat of money laundering.

Terrorism financing

Table 53

Type of used services, financial products	Precious stones and metals
General risk description	Precious stones and metals robbed by the terrorists are smuggled to the other countries for sale
Risk occurrence scenario (i.e. possible risk occurrence example)	1. A bank account of a company C was credited with relatively high amounts of money from the entities involved in diamond trading. The funds were then transferred to the Middle East for the benefit of a citizen of one of the European countries – person A originating from Africa. A part of funds was transferred via the account of one of the directors of company C. Money was converted to EUR and then transferred for Mr B. Mr A and B have purchased diamonds from the rebels operating in one of the African countries and then smuggled them to Europe. 2. Purchase of precious metals, such as gold, by a Polish company from a foreign company intermediating in trade in precious metal. Precious metals may originate from the area covered by the activity of terrorist groups and the funds from their sale may be allocated for their financing.
Level of vulnerability	3
Justification for the level of vulnerability	Although purchase and sale of relatively small amounts of such type of goods makes no greater difficulties (e.g. in the jewellery stores), it is just the opposite in the case of their large/wholesale purchase/sale. However, it is easy to avoid identification, in particular when purchasing/selling the goods of the value below the equivalence of EUR 15 thousand. It is possible to buy/sell via Internet, and therefore make transactions of international nature (for example when purchasing stones or metals from a foreign entity). At present, the entities operating in the area of trade in precious or semi-precious metals or stones are not the OIs, provided that they do not accept or make payments for the goods in cash of the value equal to or exceeding the equivalence of EUR 10 thousand, regardless of whether the transaction is made as a single or several operations which seem interlinked, or provided that they do not conduct a currency exchange activity in the field of purchase and sale of FX gold and platinum. Poland enables purchase of gold in the form of bars and gold coins – so called bullion coins (without any numismatic value). Apart from that, the bullion coins are treated as a legal tender, which enables their transportation between the countries. In addition, import, processing and trade in diamonds is not a legally regulated activity, which means that it requires neither permit nor licence nor any other decision of a public administration authority. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	1
Justification for the level of threat	Using the trade in precious stones and metals robbed by the terrorists is one of the identified methods of terrorism financing. Precious stones or metals are smuggled by the terrorist organisations from the war zones, where these organisations operate, to the other countries with the intention of sale for terrorist activity purposes. This method of financing frequently requires preparation of false certificates of origin for the sold goods. It is not entirely safe, since it may attract interest of the services of the country of sale. Using this *modus operandi* requires knowledge of the local market, planning and specialist knowledge at a medium

	level. There is no information on the possibility of using this method to finance the terrorist activity in Poland. CONCLUSION: Using the mechanism of purchasing precious stones and metals from the persons involved in terrorist activity for the purposes of terrorism financing poses a low threat in Poland.

Table 54

Type of used services, financial products	Antiques and works of art
General risk description	Purchase of stolen antiques and works of art from the persons involved in the activity of terrorist nature
Risk occurrence scenario (i.e. possible risk occurrence example)	Purchase by the Polish collectors of the works of art and antiques originating from the areas covered by the activity of terrorist organisations (for example Middle East). The purchased good could be illegally taken from their owners by a terrorist organisation to finance its activity.
Level of vulnerability	3
Justification for the level of vulnerability	Purchase/sale of antiques or works of art is relatively easy. There are many companies trading in this type of goods under the *Act of 6 March 2018 – Business Operators' Law* (auction houses, antique shops). It is possible to purchase/sale via Internet, and therefore make transactions of international nature. An important instrument, which has extended the spectrum of purchasing/selling the works of art on the market, including the international market, are the NFTs. Currently, functioning of so called *non-fungible tokens* is not regulated (the EU authorities pursue to adapt the legal regulations to this blockchain technology-based instruments). A subjective value of NFTs and lack of control over this instrument creates room for abuses in this field. At present, the operators trading or intermediating in trade in the works of art, collectors' items and antiques as well as operators providing the services of storage of works of art., collectors' items and antiques, if such activity is performed with the use of so called free port, for transactions of the value equal to or exceeding the equivalence of EUR 10,000, regardless of whether the transaction is made as a single or several operations which seem to be interlinked – are the obligated institutions in the meaning of the AML/CFT provisions. The provisions on business activity consisting in trading in the works of art. and additional regulations (among others application of the AML directive and the need of keeping the record of historical objects accepted or offered for sale) impose strict obligations on the Polish market sellers, resulting in a precise identification of all parties to the transaction and transparency of the entire sale process, including the identification of the source of origin of the item. The existing and one of the most restrictive provisions on export and import of antiques compared to the European and global legislation provide the legally operating business entities have a full record of items imported and exported from the country. The activity consisting in trading or intermediation in trade in the works of arts, collectors' items and antiques acquired and smuggled from the areas of warfare in Ukraine remains however a great unknown. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2

Justification for the level of threat	Using the mechanism of purchase of stolen antiques and works of arts from the persons involved in the activity of terrorist nature is one of the method of terrorist activity financing. According to the expert assessments, one of the basic sources of ISIS financing was the theft and sale of the ancient works of art from Syria and Iraq. The scale of works of art smuggling from the areas of warfare in Ukraine remains unknown to date. The method of terrorism financing by trade in stolen antiques and works of art is however relatively difficult to apply. It requires significant expenditure for logistics, specialist expert opinions, knowledge of the works of art market, knowledge of the customers willing to purchase goods on a black market and each trading operation should remain discrete. In many cases, it requires preparation of false certificates of origin for the antiques and works of art being sold. The performed financial operations may raise suspicions as to their legality. Using this *modus operandi* requires planning and highly specialist knowledge. There is no information on the possibility of using this knowledge to finance the terrorist activity in Poland. CONCLUSION: Using the mechanism of purchase of stolen antiques and works of arts from the persons involved in the activity of terrorist nature for the purposes of terrorism financing poses a medium threat in Poland.

Vulnerability

The high-value goods market is a broad term. It covers both the market of works of art, antiques, historical items, bibliophile, numismatic, jewellery, gold, silver and precious metals, etc.

The number of studies pertaining to this area is relatively low. This study is based on information of the Scientific and Research Working Group for Trade in the Works of Arts and Legal Protection of Cultural Heritage of the Faculty of Law and Administration at the Adam Mickiewicz University in Poznan headed by Prof., PhD Wojciech Szafrański. This information refer mostly to the works of art market.

According to this information, the Polish art market consists of the primary market characterised by the flow of the works of art from the artists to the collectors and of the secondary market, on which the previously purchased works of art are sold. A vast majority of traded goods are the Polish works of art or linked with Poland.

The Polish works of art market was built under the bottom-up approach, by the Polish capital entities. This sector has been formed without any state support and in the conditions of no interest of the political environment in the issues of market regulation. The market features imbalance caused by capital domination of large auction houses. This is manifested among others by blurring the boundaries between the primary and secondary market, expressed among others by organisation of auctions of so called young art works by large entities from the secondary market.

There is no information, how many entities actually operate on the market. The existing data point out at between 200 and 600 entities. Data provided by the Scientific and Research Working Group for Trade in the Works of Arts and Legal Protection of Cultural Heritage of the Faculty of Law and Administration (hereinafter: Working Group) indicate more specific number of art dealers in 2021 – nearly 380 entities. No data include the persons occasionally selling the works of art and these, for whom the sale of works of art is actually the main form of earning, but they do not register the activity in this field. The latter category of persons remains beyond any control, despite generating a continuous movement on the market.

There is also no certainty on the volume of turnover on the market. The existing data are only the estimates. No institution collects them in the comprehensive and covering all transactions manner. According to the Working Group data covering a broad range of information, volume of turnover on the works of art market for most involved institutions may be estimated – in the years 2019 – 2021 , for PLN 467.5 million, 561.8 million and 838.6 million, respectively. Unquestionably, the value of the Polish market of the works of art has been growing year-to-year. This growth is also manifested by placing the two Polish entities in the first fifteen largest auction houses in Europe in terms of volume of turnover.

There are no relevant regulations concerning the recording of the sale process, their integrity and responsibility. The market expert profession also remains unregulated. There is a significant number of document templates and certificates functioning on the market, which ultimately are of no actual importance.

A self-forming market has developed a number of specific methods of action. One of them is making transactions without formal agreements in writing. Uncontrolled market development resulted in the loss of transparency and impairment of the capacity to assess authenticity of the items and reliability of prices. All this takes place in the conditions of unlimited trust of the customer to the dealers.

The Working Group information referred to above apply to the works of art market, however correspond also to the remaining segments of the high-value goods market. There is no actual control over trade in both collectors' items, precious stones, historical objects, etc.

The outbreak of war in Ukraine resulted in the increased threat of inflow of high-value goods of unknown origin. Even before the war, trafficking of historical items[82], coins[83] and works of art[8485] through the border has been a significant issue of concern. A rapid inflow of the refugees, frequently transporting their personal property and not controlled in any way whatsoever, has undoubtedly lead to the increased volume of such goods in trade.

Threats in the sector

The sector of trade in high-value goods generates a significant risk both in the scope of AML/CFT and predicate offences.

Information provided by the Working Group indicate numerous problems specific for the Polish art market, for example no regulations of the valuer profession enables manipulating the value of goods. The same effect may apply to lack of control over the sale of the works of art. There is no formal mechanisms of supervision for example of the process of sale on the auctions, when enhancing the price of a given work of art is potentially possible. This issue of concern has been raised by many art market experts[86], describing the phenomenon of announcing the end of auction of a given work of art by obtaining a record price of sale, despite the fact that no

[82]https://www.gov.pl/web/kas/przemyt-463-zabytkow-archeologicznych, access on: 23.01.2023,
[83]https://www.gov.pl/web/kas/zatrzymalismy-przemyt-kilkuset-zabytkowych-monet, access on: 23.01.2023,
[84]https://tygodniksanocki.pl/2017/08/11/drewniana-ikona-7-kg-bursztynu-1576-szt-tabletek-zatrzymali-podkarpaccy-funkcjonariusze-kas/, access on: 23.01.2023,
[85]https://www.tvp.info/44561562/funkcjonariusze-kas-udaremnili-przemyt-zabytkowych-ikon, access on: 23.01.2022
[86]Janusz Miliszkiewicz "Agencja ratingowa dla rynku sztuki",Santander Art and Culture Law Review 1/2016 (2): p. 146

actual change of the owners of this work of art took place. These items are further offered in private sale at a reduced price.

The actual absence of the expert profession, specifically developed "traditions" and low social awareness have led to the pathology of the Polish market manifested by the presence of a large number of fakes. With reference to the above, we may recall the case of a journalistic provocation related to the "Zjawa" (*Phantom)* painting[87]. The expert opinions and certificates are most frequently prepared by the entities interested in increasing the value of the work of art[88]. Such circumstances open a large playing field to manipulate the prices and create the opportunity of frauds.

Domination of the works of Polish origin on the art market also creates the conditions for creating the speculation bubbles. Deficiency of the works of art of recognised artists has led to the increased number of so called young art auctions in recent years. Also the works of art of recognised artists are subject to regular fluctuations. In the case of absence of actual supervision over the market, this poses a real threat to certainty of trade.

A growing market of art in the form of NFTs is a separate issue of concern. The Working Group identified numerous potential threats that may occur with regard to this market, among others no fixed selling rate, easiness of exchange, differentiation of the NFT exchange platforms, large number of virtual stock exchanges, quickness of transactions and the fact that the NFTs are the bearer instruments.

It is difficult to assess, what is the level of use of other types of high-value goods, such as for example so called blood diamonds. In recent times, there has been information on the possible trade in such goods by the representatives of so called Wagner Group. The stones acquired in Africa are transported to Europe, mostly through the African countries, however also the transport with the use of official channels is suspected[89]. At the same time, Russia continues to export significant volumes of precious stones to such states as China and India. It is pointed out that a part of them may return to Europe as finished jewellery[90]. In the case of transport of precious stones from East, one cannot exclude the use of the territory of Poland for transit or legalisation purposes.

The issue of using the goods of culture robbed in the areas of warfare for the purposes of terrorism financing. The most important source of such artefacts is still the area of the Near and Middle East. Despite the ISIS has lost a vast majority of the occupied areas, the global markets are still fed with an inflow of historical items robbed in Syria and Iraq[91]. It should be noted that during its existence at the territory of a part of Iraq and Syria, the self-proclaimed caliphate has performed numerous acts of vandalism, destroying among others the Mosul Archaeology Museum. After liberation of the city, it was stated that a vast majority of collection was not destroyed but most probably illegally exported to the neighbouring states. The other findings revealed that ISIS has conducted its own archaeological works at the areas of archaeological

[87]https://www.tokfm.pl/Tokfm/7,103085,12079045,wojna-ze-zjawa-final-bezprecedensowej-prowokacji-dziennikarskiej.html, access on: 23.01.2023,
[88]Janusz Miliszkiewicz "Agencja ratingowa dla rynku sztuki", p. 148
[89]https://www.money.pl/gospodarka/handel-krwawymi-diamentami-kwitnie-sprzedaje-je-nawet-grupa-wagnera-6840248757066272a.html, access on: 23.01.2023,
[90]https://www.money.pl/gospodarka/krwawe-diamenty-putina-odzyskuja-blask-wymykaja-sie-sankcjom-6808012951693824a.html, access on: 23.01.2023,
[91]https://pideeco.be/articles/terrorism-financing-blood-antiquities-looted-aml/, access on 23.01.2023,

sites in the northern part of Iraq and Syria, in many cases covering the traces of its operations by destroying certain objects (for example the temple of Baal (Bel) and the arch of triumph in Palmyra) or demolishing the buildings, which have disturbed its operations (for example the prophet Jonah's Tomb in Mosul). The activity of caliphate in this area covered also among others the "taxation" of the other groups robbing the historical objects and development of trade in fakes of certain artefacts[92]. A similar phenomenon may occur soon in Afghanistan, where the Talibs have seized the resources of among others the National Museum in Kabul and the documentation describing the new archaeological sites[93] prepared in cooperation with the foreign institutions. Loss of access to the foreign accounts, loss of financing from the international funds and deteriorating economic condition may, in a longer time perspective, trigger the intention to use these resources. The territory of Poland may become at least the place of transit of such items or a place, in which they will be legalised.

Averaged level of threat of the sector of trade in high-value goods – ML – 2.5 and FT – 1.5

Averaged level of vulnerability of the sector of trade in high-value goods – ML – 3.0 and FT – 3.0

Estimated level of probability for the sector – ML – 2.80 and FT – 2.40

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the sector of trade in high-value goods – 2.04	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the sector of trade in high-value goods - 2.68	
1 – 1.5	Low
1.6 – 2.5	Medium

[92]Destruction or theft? Islamic State, Iraqi antiquities and organized crime, March 2020,
[93]Expert: Taliban will finance international terrorism by selling archaeological antiquities, 27.08.2021

2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the sector of trade in high-value goods for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the sector of trade in high-value goods for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the sector of trade in high-value goods for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

The obligated institutions from the sector of trade in high-value goods should implement the effective procedures related to the appropriate assessment of business relationship of the customer and obtaining information on their purpose and intended nature and should ensure on-going monitoring of the business relationships. The obligated institutions from the sector of trade in high-value goods should put attention to verification of the source of origin of the assets of their customers. .

The sector of trade in high-value goods should undertake the actions enhancing the awareness of exposure to the crime of money laundering and terrorism financing, as well as increasing the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions.

The trainings for the obligated institutions from the sector of trade in high-value goods, during which the theoretical and practical guidelines on determining the beneficial owner and the

ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be organised. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The obligated institutions from the sector of trading in high-value goods should put particular attention to the source of origin of assets as well as the source of origin of high-value goods being subject to trading, in particular with the view to their origin from the jurisdictions of higher risk of money laundering and terrorism financing. The obligated institutions should focus in particular on determination of data on the source of origin of the goods subject to trading and of the assets for which these goods are purchased.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance. The entities from the sector of trade in high-value goods should verity the documents of the traded items, in particular, in justified cases, should request the customers to confirm the submission of customs declarations for the valuable goods brought from the abroad or obtaining a relevant permits for import of the goods of culture.

A significant risk factor in the operation of the entities from the sector of trade in high-value goods is making the transactions without any formal agreements in writing. From the perspective of the obligations of the obligated institutions, lack of documentation of transaction is unacceptable. The loss of transparency on the market of high-value goods is bilaterally negative. Lack of relevant documentation of transactions is a major breach of the existing anti-money laundering and counter-terrorism financing regulations, which may result in imposing a painful financial penalty on the operators involved in trade in high-value goods. The customers who failed to document the transaction may be subject to numerous negative effects, for example inability to prove the value of the item on the basis of the purchase price (which may be of key importance for the potential claims of the customer in the case of loss or destruction of the purchased item). The appropriate risk-mitigating measures would include primarily the observance of the existing anti-money laundering and counter-terrorism financing in force. In order to mitigate the described risk, it may be necessary to adopt the provisions obliging the operators from the sector of trade in high-value goods to record the transaction in the electronic register.

The risk associated with the market of the works of art is failure to regulate the expert profession, which results in the functioning of many templates of documents and certificates, which ultimately are of no actual importance or meaning. Reducing this risk may require consideration of regulating the profession of expert of the works of art market.

13. Area – business activity (in general)

Sector description – is contained in the sub-chapter 2.2 “Non-financial market” and in the sub-chapter 7.2.2. “Vulnerability of the non-financial market”.

Risk occurrence scenarios (i.e. possible risk occurrence examples) referred to the use of legally operating business entities, the shell company scheme and legal assistance and tax advisory services for the purposes of money laundering, and the use of legally operating business entities and the shell company scheme for the purposes of terrorism financing. The description of the scenarios is presented below.

Money laundering

Table 55

Type of used services, financial products	Legal operation of business entities
General risk description	Using the existing business entities for money laundering purposes

Risk occurrence scenario (i.e. possible risk occurrence example)	1. Purposeful combining the illicit proceeds with legal revenue of a business entity involved in international trade to impede identification of the source of origin of specific assets. 2. Using the business entities, earning revenue from business activity mostly in cash (for example restaurants, hotels). Overstating the total revenue becomes a method to enter the illicit proceeds into licit economy. 3. Using the entities established abroad (holding their accounts in the Republic of Poland) to enter the illicit proceeds into licit economy. 4. Using the Polish companies with foreigners as the owners/shareholders to enter the illicit proceeds into licit economy. 5. Using the Polish companies holding the foreign accounts (kept for the residents) to enter the illicit proceeds into licit economy.
Level of vulnerability	2
Justification for the level of vulnerability	Establishing a commercial law company or starting business as a natural person running a business activity is limited by the provisions of law to a certain extent. These provisions require a registration and meeting certain conditions (for example with regard to the capital companies and limited joint-stock partnership, to have a share capital of a specific value). It is possible to hide data of the beneficial owner by using the straw men or shell companies. Contribution of the initial capital or purchase/acquisition of an already existing entity may be made by means of a financial transaction of an international nature or with participation of the foreign persons/entities. Only a part of business entities is the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information only to a limited extent, however the capacity of their quick analysing is limited by human resources deficiencies and sufficiently efficient software. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Using the existing business entities for money laundering purposes is one of the most common methods of money laundering. This method is widely available, inexpensive and perceived by the perpetrators as highly attractive. Using the existing business for money laundering purposes requires neither specialist knowledge on the banking system, nor specific specialist skills. It is frequently used by organised crime. When a crime group receives money, from example from street drug dealing, it uses the companies, which potentially earn their revenue in cash for money laundering. Inexpensiveness of the method is ensured by creative accounting and tax optimisation. The GIFI receives information on using this method for money laundering purposes. CONCLUSION: Using the existing business entities for money laundering purposes poses a very high risk of money laundering.

Table 56

Type of used services, financial products	Shell companies
General risk description	Using the companies not actually running a business activity for money laundering purposes

Risk occurrence scenario (i.e. possible risk occurrence example)	1. Purchase of companies, which have previously conducted a business activity for the purposes of using them to impede identification of transfer of illicit proceeds. 2. The perpetrators create complicated and long chains of the organisational and ownership links between the business entities, associations, charity organisations, trusts (involving the entities registered in various jurisdictions, including in tax havens) in order to impede identification of the actual owners of the entities used for money laundering purposes. 3. Transfer of funds between these entities under fictitious titles (for example purchase/sale of goods/services, shares/stocks, granting/repayment of loans) to hide their origin. 4. Using the accounting and administration services, offered by a business entities specialising in such activity, to establish and run a limit liability company used for money laundering purposes.
Level of vulnerability	2
Justification for the level of vulnerability	Establishing a commercial law company or starting business as a natural person running a business activity is limited by the provisions of law to a certain extent. These provisions require a registration and meeting certain conditions (for example with regard to the capital companies and limited joint-stock partnership, to have a share capital of a specific value). It is possible to hide data of the beneficial owner by using the straw men or shell companies. Contribution of the initial capital or purchase/acquisition of an already existing entity may be made by means of a financial transaction of an international nature or with participation of the foreign persons/entities. Only a part of business entities is the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information only to a limited extent, however the capacity of their quick analysing is limited by human resources deficiencies and sufficiently efficient software. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	4
Justification for the level of threat	Using the companies not actually running a business activity for money laundering purposes is one of the most common methods of money laundering. This method is widely available, inexpensive and perceived by the perpetrators as attractive and safe. It is frequently treated as a component necessary in the operations aimed at legitimisation of the proceeds of crime. Using the companies not actually running a business activity requires neither specialist knowledge on the banking system, nor specialist skills. In practice, only the bank accounts of such shell companies are used. A shell company may act only as an intermediary in the transaction chain, aimed at obfuscating and extending the transaction path for laundered money. On the other hand, it may act as the ultimate link in the transaction chain. A shell company may be a domestic entity, but also may be registered in a foreign jurisdiction, in particular in a “tax haven”, with restrictive provisions on the bank secrecy. The GIFI receives information on using this method for money laundering purposes. CONCLUSION: Using the companies not actually running a business activity poses a very high risk of money laundering.

Table 57

Type of used services, financial products	Legal assistance and tax advisory services

General risk description	Using other entities as the intermediaries to legitimise the illicit proceeds
Risk occurrence scenario (i.e. possible risk occurrence example)	Assisting the offenders in the transactions of purchase of real estates and high-value goods, establishment and running the business entities, foundations, trusts in the country and abroad, as well as assisting in the financial transactions by making the bank accounts available.
Level of vulnerability	3
Justification for the level of vulnerability	Access to legal assistance and tax advisory services is relatively easy. They facilitate hiding of the identification data of customers and making transactions of international nature. These service providers are the OIs. They have certain awareness of their AML/CFT obligations. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information only to a limited extent, however the capacity of their quick analysing is limited by human resources deficiencies and sufficiently efficient software. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a limited extent.
Level of threat	4
Justification for the level of threat	Using the intermediation of the other entities (in particular lawyers, tax advisors, notaries) to transfer and legitimise the illicit proceeds is one of the basic methods of money laundering. The GIFI holds information on using this *modus operandi*. The representatives of the above-mentioned professions provide the perpetrators with access to the specialist legal and tax knowledge. This may considerably enhance laundering of the proceeds of crime. The option to allocate funds onto the bank accounts owned by the lawyers, for example as a deposit, is also of importance. Withdrawal or transfer onto the other account from such account simulates legal origin of the proceeds of crime and bears all features of legitimisation of laundered funds. Using the intermediation of the legal professions or a tax adviser is also of significant due to the fact that the services offered by these professions are in some cases necessary to make a given transaction and increase their safety. Access to legal services provided by tax advisors, notaries or lawyers is relatively easy and requires neither specific skills nor specialist knowledge. This *modus operandi* is perceived by the perpetrators as relatively attractive and safe form of money laundering. CONCLUSION: using the intermediation of the other entities (in particular lawyers, tax advisors and notaries) for the purposes of transferring and legitimising the illicit proceeds poses a high threat of money laundering.

Table 58

Type of used services, financial products	Foreign bribery

General risk description	Bribery of a foreign public official[94]
Risk occurrence scenario (i.e. possible risk occurrence example)	1. An official of the Ministry of Economy in one of the African states accept the proposed material gain in exchange for positive awarding the contract to the Polish company operating on this continent. The proceeds of crime were deposited in one of the African banks and in a short period of time were withdrawn in cash by the persons holding the power of attorney for this bank account. 2. The Polish services identified several transactions in the Polish financial system, beneficiary of which was a public official of one of the EU states. This person was involved in an "unofficial" lobbing for implementation of a governmental contract by Poland at the territory of the Republic of Poland The entity (contractor) was established in the European Union state of the lobbying official. The funds were withdrawn in cash and then transported outside the Republic of Poland.
Level of vulnerability	3
Justification for the level of vulnerability	Laundering of the proceeds of crime of bribery of a foreign public official is an offence identified by the public administration authorities. The Polish public officials are obliged to report the charges of committing a crime under Article 304(2) of the Code of Criminal Procedure. Failure to observe Article 304(2) of the Code of Criminal Procedure may constitute a crime under Article 231 of the Penal Code (Abuse of function). The crime of money laundering in the case of bribery of a foreign public official is contained in Article 7 of the *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.* The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk. With regard to the pending military conflict in Ukraine as well as the future restoration of the Ukrainian state, there is a threat of bribery of foreign public officials in Ukraine by the representatives of the foreign companies wishing to obtain for example the contracts for the post-war restoration of this country.
Level of threat	4
Justification for the level of threat	Bribery of a foreign public official is a crime difficult to detect and requiring specific actions taken by the services of a given state. One should emphasize the fact that the persons performing a specific function usually benefit from so called diplomatic privileges and immunities, which prevent or impede taking the actions by the relevant services in the case of identifying this offence. It should be noted that the consequences of bribery of a foreign public official may have, in certain cases, a significant impact on the proper functioning of a given state (strategic information on such state, sensitive information etc.). The GIFI has information on using this *modus operandi*. This method of placing the illicit proceeds on the market is perceived by the perpetrators as relatively attractive and safe form of money laundering. CONCLUSION: bribery of a foreign public official poses a high threat of money laundering.

[94] a foreign public official means any person holding the legislative, administrative or judicial position in a foreign state, both appointed and elected, as well as any person performing the public functions for a foreign state, including the public agenda or public company official and any official or representative of a public international organisation

Terrorism financing

Table 59

Type of used services, financial products	Legal operation of business entities
General risk description	Using the existing business entities for terrorism financing purposes
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Company X operating on the used cars market finances the terrorism from revenue earned from sold cars. 2. Financing the activity of a terrorist organisation from revenue earned by a company involved in leasing and trade in real estates. 3. Purposeful combining of funds obtained from the sponsors of a terrorist activity with legal revenue of a business entity involved in the international trade to impede identification of the terrorism financing practice. 4. A person running a business activity in the IT sector provides the services to the customers from may countries and may work remotely. As a company, this person accepts various payment methods, such as PayPal, bank transfers, cryptocurrencies, etc. This company transfers and receives payments from the other company providing the IT services to the foreign customers. This second company is already known of its attempts to transfer the funds to a person linked with a terrorist organisation.
Level of vulnerability	2
Justification for the level of vulnerability	Establishing a commercial law company or starting business as a natural person running a business activity is limited by the provisions of law to a certain extent. These provisions require a registration and meeting certain conditions (for example with regard to the capital companies and limited joint-stock partnership, to have a share capital of a specific value). It is possible to hide data of the beneficial owner by using the straw men or shell companies. Contribution of the initial capital or purchase/acquisition of an already existing entity may be made by means of a financial transaction of an international nature or with participation of the foreign persons/entities. Only a part of business entities is the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information only to a limited extent. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2

Justification for the level of threat	Using the existing business entities for terrorism financing purposes is one of the basis methods of financing of terrorist activity. Legally operating companies act for the benefit of the terrorist organisations, and a part of all profits of these companies is transferred for a terrorism-related activity. These companies operate usually in the sectors related to trade in real estates, electronic products, used cars, precious metals, textiles, export and import of food and gastronomy). Legally operating companies may be used for direct acquisition of funds supporting the terrorist activities or as a "conveyors" transmitting duns related to financing of such activities. The legally earned revenue of a business entity is frequently blended with the funds obtained from the terrorism financing sources and transferred further in order to impede identification of funds as supporting the terrorism. The legally operating companies involved in transfer of funds linked with terrorism financing are frequently run by the members of one ethnical groups, which increases difficulties in the identification of this practice. This is a relatively easy and widely available method, quite inexpensive and perceived by the perpetrators as relatively attractive. Using the operating business entities for terrorism financing purposes usually raises no suspicions. High volume of turnover of the companies concerned allows hiding the use of these companies for transferring the funds for the purposes of terrorist activity, in particular when the one-off amounts are not too high. The beneficial owner is frequently hidden using falsified transaction documentation. Using this *modus operandi* requires however planning, accounting knowledge and logistical skills. In the Europol TE-SAT report for 2020, Poland noted that contributions for the activity of right-wing extremist groups originate from the members of these groups running legally operating private companies. The GIFI has received little information on the opportunities to use this method for financing of terrorist activity. CONCLUSION: Using the existing business entities for terrorism financing purposes poses a medium threat in Poland.

Table 60

Type of used services, financial products	Shell companies
General risk description	Using the companies not actually running a business activity for terrorism financing purposes.
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Purchase of companies, which have previously conducted a business activity for the purposes of using them to impede identification of transfer of assets aimed at terrorism financing. 2. Providing the accounting and administration services to a limit liability company owned by a foreigner by a Polish business entities specialising in services for the enterprises. Using the limit liability company concerned for the purposes of terrorism financing. 3. The perpetrators create complicated and long chains of the organisational and ownership links between the business entities, associations, charity organisations, trusts (involving the entities registered in various jurisdictions, including in tax havens) in order to impede identification of the actual owners of the entities used for terrorism financing purposes. 4. Transfer of funds between these entities under fictitious titles (for example purchase/sale of goods/services, shares/stocks, granting/repayment of loans) to finance the needs of the terrorists.
Level of vulnerability	2

Justification for the level of vulnerability	Establishing a commercial law company or starting business as a natural person running a business activity is limited by the provisions of law to a certain extent. These provisions require a registration and meeting certain conditions (for example with regard to the capital companies and limited joint-stock partnership, to have a share capital of a specific value). It is possible to hide data of the beneficial owner by using the straw men or shell companies. Contribution of the initial capital or purchase/acquisition of an already existing entity may be made by means of a financial transaction of an international nature or with participation of the foreign persons/entities. Only a part of business entities is the OIs. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information only to a limited extent. It is highly probable that the case of FT in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	2
Justification for the level of threat	Using the companies not actually running a business activity is one of the basic methods for transferring funds linked with financing the terrorist activity. Legally established, yet not operating in practice companies, use several accounts only as the "conveyors" to transfer the funds to the terrorist organisations. Deposits in cash or transfers made to the company aim at obfuscating the origin of the funds, which are transferred further, frequently onto the accounts of the other entities situated in the sensitive areas in terms of countering terrorism. In many cases, these shell companies involved in the flow of funds linked with terrorism financing are run by the members of a single ethical group, which increases difficulties with the identification of this practice. Using the companies not actually running a business activity for transfer of funds linked with financing the terrorist activity is a relatively easy and widely available method, is inexpensive and may be perceived by the perpetrators as relatively attractive. Using the operating business entities to finance terrorism usually raises no suspicions, however a noticeable non-standard business approach of these companies poses sometimes a threat. The beneficial owner is frequently hidden using falsified transaction documentation. Using this *modus operandi* requires however planning, accounting knowledge and logistical skills. The GIFI has received little information on the opportunity to use this method for financing of terrorist activity. CONCLUSION: Using the companies not actually running a business activity for terrorism financing purposes poses a medium threat in Poland.

A basic principle expressed directly in the *Act of 6 March 2018 – Business Operators' Law* is the principle of freedom of business activity. This means that taking up, conducting and terminating the business activity is free for everyone on equal rights. Only conducting of a business activity in the areas of particular significance due to the security of the state or citizens, or any other overriding reason of public interest, when it cannot be conducted as free, it requires obtaining a relevant licence, permit or entry into the register of regulated activity. According to the Polish legislation, an operator is any natural person, legal person or organisational unit other than legal person granted with legal capacity under a separate act, as well as the partners of a civil-law company in the scope of the performed business activity, conducting a business

activity. Business activity can be started on the day of applying for entry into the Business Activity Central Register and Information Record (CEIDG) or upon making the entry to the register of business operators of the National Court Register (KRS), unless the specific provisions state otherwise. A capital company in organisation may start a business activity before entering into the register of business operators.

A business activity in Poland can be conducted in various legal forms. In the event of an individual business activity and civil law companies, the place of registration of the activity is the Business Activity Central Register and Information Record (CEIDG). For the remaining legal forms, the place of registration is the National Court Register (KRS). The National Court Register consists of the register of business operators; register of associations, other social and professional organisations, foundations and public healthcare facilities; and of the register of insolvent debtors.

As of the end of December 2022, Statistics Poland (GUS) estimated the number of entities conducting a business activity for 4,986,256[95]. This does not mean however that there are currently nearly 5 millions of active companies. The Statistics Poland statistical data include also the entities, which suspended or terminated the activity, but such information was not submitted to the Statistics Poland, and the entities being not the business operators (foundations, associations). The register of business operators covers the following entities: general partnerships; European Economic Interest Groupings; professional partnerships; limited partnerships; limited joint-stock partnerships; limited liability companies; joint-stock companies; European companies; cooperatives; state enterprises; research and development units; business operators listed in the provisions on the rules of conducting of business activity in field of small-scale production by the foreign legal and natural persons at the territory of the Republic of Poland; mutual insurance companies; other legal persons, if they conduct a business activity and are subject to mandatory entry into the register; branches of foreign businesses operating at the territory of the Republic of Poland; main branches of the foreign insurance companies.

The entity obliged to apply for entry into the Register cannot refer towards any third persons, in good will, to data, which have not been entered into the Register or were deleted from the Register.

At the same time, according to analyses performed by the National Economic Information Centre (Centralny Ośrodek Informacji Gospodarczej)[96] , as of 11 August 2022 there were 93,258 companies with foreign capital share or with beneficial owners being the citizens of the other states operating in Poland. Each year, between 6,000 and 10,000 new foreign capital companies are established.

In 2015, there were 6,706 such companies established, in 2016 – 7,122, in 2017 – 7,282, in 2018 – 7,878, in 2019 – 8,820, in 2020 – 6,924, in 2021 10,494, while by the end of June 2022 – 5,581 companies. Each year, 3,500 – 4,000 companies change the owners from Polish to the foreign ones. In addition, nearly 60% of all active foreign companies were established in the

[95] https://stat.gov.pl/Areay-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/miesieczna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-grudzien-2022,4,65.html, access on 30.01.2023

[96] https://www.coig.com.pl/inwestorzy-zagraniczni-w-polsce.php, access on 30.01.2023

last 5 years. Most of these companies were established with participation of the Ukrainian (23,259), German (8,936) and Belarusian (4,025) citizens.

According to the analyses performed by the National Economic Information Centre (Centralny Ośrodek Informacji Gospodarczej), in 2022 there were 55,447 new entities registered in the Register of Business Operators of the National Court Register, which is by 1.51% less compared to 2021. At the same time, the Official Court and Economic Journal and the National Register of Debtors published 360 bankruptcies of the companies.

The greatest number of active foreign capital companies in Poland operates in the legal form of the limited liability company, which accounts for 94.14%[97]. The core activity of vast majority of these companies was road transport – 4,553 companies; construction of buildings – 3,759 companies; other advisory services – 3,462 companies; wholesale – 3,374 companies. Vast majority of foreign capital companies have their seat in Warsaw.

In 2021, the non-financial companies earned[98] PLN 6,287.7 billion of total revenue, generated PLN 1,448.7 billion of added value, and the value of their production amounted to PLN 4,662.0 billion. Nearly a half of value in the above-mentioned categories was generated by large entities. Compared to 2022, the value of total revenue of non-financial companies increased by 19.6%. In terms of the type of conducted activity, 72.9% of total revenue was generated by the industrial and trade companies jointly. Gross financial result of non-financial companies in 2021 amounted to PLN 569.3 billion and was higher by PLN 210.3 billion (i.e. by 58.6%) compared to 2022. The highest gross financial result in 2021 was generated by the industrial companies (PLN 185.4 billion, of which PLN 145.2 billion were recorded in the industrial processing entities), while in terms of location – the entities with their seat in the Mazowieckie Voivodeship (29.0% of share).

Vulnerability of the sector

The crime of money laundering is the practice of legalising the illicit proceeds or the proceeds from unknown sources by their placing on the market, which poses a threat to its proper functioning. As a process extended over time, this practice frequently covers the subsequent stages of the activities with the ultimate objective of integration of the illegal proceeds with the capital obtained from legal sources, which creates the opportunity of using the "cleaned" funds legally. The crime of money laundering was recognised by the legislator as the crime separate from a predicate offence (being a potential source of illegally legalised benefits), and the legislator imposed severe penal sanctions for this crime, in many cases exceeding the threat provided for the predicate offences. Money laundering is an independent type of an offence. Article 299 of the Penal Code penalising money laundering is introduced in Chapter XXXV of the Code, which covers the crimes against economic activity (penalisation of money laundering was initially introduced to the *Act of 12 December 1994 on the protection of economic activity and amendment of certain provisions of the criminal law*. Although the criteria of the crime of money laundering laid down in the Code do not indicate the breach of this legal interest directly,

[97] Ibidem.

[98] Analysis of the Statistics Poland entitled: Działalność przedsiębiorstw niefinansowych w 2021 r., Warsaw 2022 - https://stat.gov.pl/Areay-tematyczne/podmioty-gospodarcze-wyniki-finansowe/przedsiebiorstwa-niefinansowe/dzialalnosc-przedsiebiorstw-niefinansowych-w-2021-roku,2,18.html, access on 02.02.2023

the most important object of protection in the case of the crime of money laundering set out in Article 299(1) of the Penal Code is the properness of business activity[99].

One of the most commonly used methods of money laundering is so called blending. This method consists in blending the illegal proceeds with legal income. To this end, the offenders establish a business activity, which should feature certain properties, such as trade in cash, difficulties in determining the amount of actual income, large dynamics of changes in the amount of revenue and number of customers. In addition, this should be a service activity, to avoid the need to indicate a specific and easily quantifiable production. The best types of business activity include the restaurants, cafes, scrap yards, discos and solaria. In many cases, the transfer of funds takes place via a bank account of natural persons conducting a business activity or other business entities. The bank accounts of business entities are credited with low and higher amounts and then are transferred onto the accounts of the other entities, frequently located in so called tax havens. The nature of financial operations on the accounts of business entities linked with money laundering features in general no significant differences compared to the ordinary and legal financial and commercial activities in trading.

One should also note that due to the existing regulations on the information obligations of the quoted companies, such companies are slightly less vulnerable to both money laundering and terrorism financing. Obligation of publication of the interim financial statements is laid down in the generally applicable laws in Poland and rules and regulations of the stock exchanges. In each case, the content of interim financial statements is defined in details and each type of the statement contains both financial data and descriptive information, which presents the operation and business environment of a given company in the reported period. The interim financial statements should reflect the existing market position of a given company and be prepared in a true, reliable and complete manner.

With regard to the activity of the business activities suspected of money laundering, in many cases the existence of family relationships between the members of the management bodies of the commercial law companies needs to be taken into account. Transactions between the subsidiary entities are possible. The results may include for example acting to the detriment of the company by the president of the management board, in effect of which a part of assets will be transferred onto the account of a subsidiary company. The most typical symptoms of application of this method may include:

- frequent transactions in relatively low amounts between the companies owned by each spouse, relative,
- repeating creditings of a bank account under the title of “donation”, “loan”, “loan reimbursement”, “debt reimbursement”,
- transactions between the accounts of the persons of the same surnames and between the accounts, analysis of which revealed that the owners or authorised representatives are related.

Despite the principle that the financial operations on the accounts of business entities linked with money laundering are similar or identical as the transactions in the normal course of business, the forms of additional business entities used for the purposes of money laundering

[99] RESOLUTION concerning the composition of seven judges of the Supreme Court of 18 December 2013, case file and KZP repertory no. 19/13.

are highly specific. These include the offshore and shell companies. According to the responses of the cooperating units concerning the GIFI survey carried out in August 2021 for the obligated institutions and cooperating units, from among 5 products and services offered outside the financial market most frequently mentioned by the cooperating units, the business entities with their seat in so called tax or financial havens were considered the third most exposed entities to money laundering.

An offshore company is a company, usually a capital company or of such nature, registered in the country, in which it conducts no business activity. The offshore companies are usually registered in tax havens. The registration can be remote, without the obligation to appear in the office personally. The benefits from registering such company include primarily the confidentiality of information, tax advantages and the protection of assets. The names of the owners of the offshore companies are secret and difficult to trace. One should note that an offshore company does not need to be illegal, if its existence is reported to the competent state authorities. The offshore jurisdictions usually impose tax only on income earned at the territory of this state. Since these jurisdictions have implemented no taxes on capital gains, real estates, donations or inheritances, establishment of the offshore company usually enables avoiding such taxes. Establishing such company does not encounter major obstacles apart from administrative fees, hiring the managers/registration representatives, etc. Since these companies conduct no business activity in the country of registration, they do not need to organise the shareholder meetings or hire any employees. Usually there is also no obligation to present the annual financial statements.

Apart from the offshore companies, another form of illicit use of the entities for the purposes of predicate offences and money laundering are so called shell companies. These are the entities, in which – in exchange for relative small financial gains – the natural persons (figureheads, straw men) agree to use their personal data to register these business entities and open the bank accounts, which are further used for money laundering. In the case of shell companies, a significant element of such actions is enabling access to the bank accounts using the electronic communications means (in particular via Internet). The transaction orders and other business instructions on behalf of the company are actually placed by the persons not authorised to act on its behalf. The activities of shell companies facilitate hiding data of the actual ordering parties of the transaction and prevent application of the relevant customer due diligence measures by the obligated institutions in due time. The fuel and scrap companies are particularly exposed to the operation of shell companies, which involved the “missing trader” frauds, carousel frauds, issuing “blank invoices” or incurring credits and loans.

The public administration authorities have knowledge on the ML/FT risk in the scope of the sector concerned. The GIFI is capable to collect and analyse information only to a limited extent. It is highly probable that the case of money laundering or terrorism financing will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

In terms of assessment of the threat of money laundering and terrorism financing, the business activity sector is the sector that can be potentially used for the predicate offences for money laundering and terrorism financing. The offshore companies participating in economic activity pose a particular threat from the perspective of both money laundering and terrorism financing. Their integration in the transaction chain contributes to losing the transaction trace of suspicious transactions (in particular in the international trade transactions). High level of confidentiality or even anonymity of the beneficial owner of the entities, to which the offshore companies belong, impede or prevent analysis of the actual business relationships of a specific entity or determination of its true structure, purpose and intended nature of transactions. In terms of threat, one should also note that the offshore companies usually have fast registration proceedings and relatively low fees. Their establishment and integration into trade is a matter of days, or even hours. According to the experience, may offshore companies have been used to hide the proceeds of crime, both of organised crime and terrorism.

The shell companies pose a similar threat from the perspective of money laundering and terrorism financing. Hiding data of the actual transaction ordering parties makes the relationships between the actual owners of legal funds subject to trading and the illicit proceeds entered onto the market non-transparent. Using a chain of legal companies and shall companies and their bank accounts in the economic activity, as well as using the intermediation of many obligated institutions in the transactions significantly impedes the verification of transactions with the aim to identify the beneficial owner by the obligated institutions and authorised authorities. This is additionally deteriorated in the event of making the business transactions between several jurisdictions.

In terms of assessment of the threat of money laundering and terrorism financing, the business activity sector is the sector that can be potentially used for the predicate offences for money laundering and terrorism financing. There are many methods of using the business activity for money laundering or terrorism financing, which can be generated in many areas.

These methods may include for example a simple transfer of funds using the bank accounts held by the business entities. The bank account is credited with cash (for example from the service companies. The following procedures shall apply: structuring – dividing the payments onto bank accounts below the above-threshold values; smurfing – i.e. fragmenting of payments by using many straw men and blending – i.e. mixing of dirty and clean money). The second stage of money laundering is making the funds available to the real beneficiaries abroad. In such cases, hiding the origin of the funds and their intended transfer abroad takes place with the use of the accounts of straw men or shell companies. Such scheme is very difficult to apply in the case of quoted companies due to their information obligations. The business reports are published on the dates laid down by the law, which is for example 4 months for annual reports, 3 months for semi-annual reports and 60 days for quarterly reports – starting from the end date of the reporting period.

Another money laundering business entity is potentially the currency exchange office involved both in purchase and sale of foreign currencies. The currency exchange office can be operated practically in any legal form provided for by the Polish legislation, yet it requires the entry into the register of currency exchange activity kept under the supervision of the National Bank of Poland. For a company operating on the market, establishing and running a currency exchange office is not difficult. It is possible to open the currency exchange office to create a money

laundry for illicit proceeds. Such currency exchange office running a business activity of trading in foreign currency could at the same time legalise the illicit proceeds by recognising them as revenue from the activity.

The organised crime groups may also launder money using the donations and loans set out in the Civil Code. In such case, a legal person earning illegal profits and wishing to legalise them, makes an arrangement with the other persons and prepares a fictitious loan or donation agreement and registers it in the tax office, paying a due tax. This method of money laundering in the form of a loan or donation between the entities is frequently used by the entities registered in so called tax havens.

Also the factoring agreements can be used for money laundering in business activity. In this case, the crime groups e.g. open usually legal companies, which in turn conduct a fictitious activity coming down to a fictitious invoicing of sale, which has never taken place, incurring fictitious liabilities acting as a formal basis for recoveries.

According to the GIFI data on the notifications of suspected crime of money laundering submitted by the GIFI to the public prosecutor's office between January 2019 and August 2022, more than 39% of natural persons conducting a business activity in Poland being the entities listed in the GIFI notifications are the Polish citizens. The largest group accounting for more than 50% of this statistic, is the persons conducting a business activity without an assigned citizenship. The other nationalities recorded in the Business Activity Central Register and Information Record (CEIDG) include the citizens of Ukraine -2.75%, Vietnam – 1.65% and Latvia – 0.82%.

In the total number of notifications of suspected crime of money laundering submitted by the GIFI to the public prosecutor's office between January 2019 and August 2022, the highest share was recorded among the natural persons – 48.44%. The other entities listed in the GIFI notifications, the highest share was recorded among the limited liability companies – 28.78%, followed by foreign companies – 9.33% and natural persons conducting a business activity – 4.59%.

Business activity can be also one of the methods of terrorism financing. The funds may originate both from legal activity and shadow economy. Income from legal activity allocated to terrorism financing originates primarily from these sectors of business activity, starting of which imposes no formal requirements on the qualifications related to a given profession or activity and requires no significant investments. The risk that the company will transfer the funds for terrorism supporting is greater, when the link between the recognised sale and actual sale is difficult to verify and in the case of capital-intensive activity. The most commonly known and described in the literature case of terrorism financing from income from a business activity was the international chain of the companies owned by Osama bin Laden. According to the Europol TESAT 2022[100] report, the terrorist and extremist organisations have been actively financed by the organisations of commercial events (a form of business activity). Despite difficulties during the COVID-19 pandemic, some groups have collected funds in this manner. This applied in particular to the extremist right-wing, left-wing, ethnical-nationalistic groups and separatist groups. In this case, the income is the profits from the sales of tickets, promotional actions and donations. The authors of the TESAT 2022 report assessed that such volume of income of these

[100] https://www.europol.europa.eu/publications-events/main-reports/tesat-report, access on 02.02.2023

groups is however insignificant. In addition, the left-wing extremists carry out their traditional sale of books and dedicated journals for the purposes of funds collection. The other income generating methods include also the online sale of goods on the e-commerce platforms (bands t-shirts, CDs and nazi items from the WWII period in the right-wing context).

Also in Poland, income from the performed work (both legal and illegal) intended for terrorism financing, are the subject of the Internal Security Agency (ABW) proceedings. According to the GIFI information, the Internal Security Agency, during its operational and analytical activities, has identified this method of collecting and transferring of funds aimed at support of the terrorist organisations.

Averaged level of threat of the business activity sector – ML – 4.0 and FT – 2.0

Averaged level of vulnerability of the business activity sector – ML – 2.5 and FT – 2.0

Estimated level of probability for the sector – ML – 3.10 and FT – 2.00

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the business activity sector – 1 .80	
1 – 1 .5	Low
1 .6 – 2 .5	Medium
2 .6 – 3 .5	High
3 .6 – 4	Very high
ML risk of the business activity sector – 2 .86	
1 – 1 .5	Low
1 .6 – 2 .5	Medium
2 .6 – 3 .5	High
3 .6 – 4	Very high

CONCLUSION 1: The level of risk of using the business activity sector for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the business activity sector for the purposes of money laundering in Poland is at a high level.

Mitigation of the identified risks:

In order to mitigate the probability of using the business activity for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions. The operators not covered by the previous sections are partially the obligated institutions. This applies in particular to the operators in the area of legal assistance, notary services, tax advisory or trade in real estates. Their awareness of threats related to money laundering and terrorism financing remains at a diversified level. The proposed mitigating measures should be implemented with consideration to the risk identified by the obligated institution concerned.

With regard to the activity of the obligated institutions involved in provision of broadly understood legal assistance services, there is a risk related to reluctance of the obligated institution to break a specific loyalty of the operator to the customer. Reducing this risk is linked with the need to prepare the dedicated training programmes for the obligated institutions operating in the above-mentioned sectors.

The obligated institutions involved in the provision of broadly understood legal assistance services should put particular attention to verification of the source of origin of the customers' assets.

The obligated institutions should put particular attention to the business relationships linked with the jurisdictions characterised by the higher risk of money laundering and terrorism financing. The obligated institutions involved in the provision of broadly understood legal assistance services, should analyse the legitimacy of establishing the business relationships with the customers from third states. The obligated institutions providing the notary services should verify the source of origin of assets, in particular in the case to transactions of the contractors from the third states.

The obligated institutions should put a particular emphasis on obtaining information from the customer on the purpose and intended nature of business relationships and should monitor the business relationships on an on-going basis and, in justified cases, request the customer to provide information and documents on the source of origin of assets. Performing the assessment of economic justification of the performed activities is reasonable especially when the obligated institutions from sector of notary services covering the disposal of enterprises or contributing to the capital companies. The obligated institutions should put particular attention to obtaining relevant up-to-date information on the customer and in the course of business relationships also on the transactions made for and by the customer. The obligated institutions should undertake the actions enhancing the awareness of exposure to the crime of money laundering and terrorism financing, as well as increasing the level of sectoral staff skills in the area of analysis of warning signals stemming from the suspicious transactions. The obligated institutions providing the accounting services or tax advisory services should draw attention to identification of boundaries between a reasonable cost optimisation by the customers and the crime of tax fraud as well as further activities constituting the laundering of money obtained from tax frauds.

It is recommended to develop the advanced IT tools and systems supporting the implementation of the objectives of anti-money laundering and counter-terrorism financing and deploy such solutions by the entities, which have not used them yet.

The trainings for the obligated institutions from the payment services sector, during which the theoretical and practical guidelines on determining the beneficial owner and the ownership and control structure of the customers and on reporting the discrepancies to the authority competent for the Central Register of Beneficial Owners (CRBO) are provided, should be continued. Participation of the representatives of the obligated institutions in the trainings raising the AML/CFT awareness, organised both by the GIFI and by the Office of the Polish Financial Supervision Authority (PFSA) under the CEDUR Programme, is recommended.

The obligated institutions should put particular attention to the geographic factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years. Due to high risk of transferring the proceeds from illicit trade, human trafficking, arms trafficking, or actions aimed at avoiding the economic sanctions, analysing by the obligated institutions of both data related to the transaction parties and to the beneficial owners, or actual purposes of specific transactions, is of particular importance.

The obligated institutions should put particular attention to the basis of a given transaction, in particular to confirm that the transactions are compliant with knowledge of the obligated institution on the customer. This applies also to the obligated institutions from the sector of the designated non-financial operators and professions, which do not make a given transaction, but provide services for the customer, under which they provide legal or accounting assistance for the transaction.

With regard to the obligated institutions from the sector of designated non-financial operators and professions, it is reasonable to develop the scope of training activities in order to increase the level of awareness of importance of these institutions for the entire anti-money laundering and counter-terrorism financing system.

14. Area – Real estates

Sector description – is contained in the sub-chapter 2.2 “Non-financial market” and in sub-chapter 7.2.2. “Vulnerability of the non-financial market”.

Risk occurrence scenarios (i.e. possible risk occurrence examples) referred to the use of various forms of transfer of ownership of the real estates, forms of property securities on real estates and contributions in-kind to the companies for the purposes of money laundering, and the use of sales of real estates and lease of owned real estates for the purposes of terrorism financing. The description of the scenarios is presented below.

Money laundering

Table 61

Type of used services, financial products	Transfer of ownership of real estates
General risk description	Using various forms of transfer of ownership of real estates for money laundering purposes
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Purchase of fixed assets by the company was secured with the entry to the mortgage register of real estates. Since the company was a subsidiary company, the instalments were paid by the parent company actually owned by the members of a crime group. In effect of an agreement between the companies, the purchased fixed assets were brought out from Poland. 2. An entity purchases a real estate for an understated price compared to the market price. The difference in the amounts in relation to market price is paid to the seller outside the agreement. Upon the expiry of a certain period of time, the real estate is sold at the market price with a recognised profit. 3. Making the purchase/sale transaction of the same real estate among the group of interlinked persons. The overstated prices of real estate are financed from the proceeds of crime. Overstating the price of real estate becomes a method for introducing the illicit proceeds into licit economy. 4. Purchase of real estates for the funds obtained from the bank mortgage loan. The instalments are paid with the illicit proceeds. 5. Exchange of one real estate to several other real estates, proper price of which is difficult to determine. The difference in the value of exchanged real estates combined with the immediately following transaction of sale is used for introducing the illicit proceeds into licit economy. 6. Purchase of real estate for the illicit proceeds. Purchase/sale of real estate takes place by submitting false statements and documents to the notary by the parties to the transaction, concerning the form of transfer of funds. Instead of payment on the bank account of the developer, the entire amount or its larger part is paid by the purchaser in cash from criminal activity.
Level of vulnerability	2
Justification for the level of vulnerability	Transfer of ownership of real estates is possible in many forms: sale, exchange, donation, inheritance or life estate contract. In order to make transfer of real estate effective, a notary deed needs to be signed. Without such deed, the concluded agreement shall have no legal effect. The sale is always a form of transfer of ownership of the real estates made against payment. Under the exchange agreement, each party obliges itself to transfer onto the other party the ownership of the good in exchange for obligation to transfer the ownership of the other good. The specific procedures apply when purchasing a real estate from a developer, when a purchaser obliges itself to purchase an apartment before the building is actually erected. In such case, two notary deeds are signed (developer and promised contract). The basic evidence of existence of the ownership right of a real estate is the mortgage register. The GIFI has relevant access to the system of Electronic Mortgage Registers. Apart from the notary, the transfer of ownership of a real estate may involve the real-estate agents, as well as the advocates, legal councillors and lawyers from the abroad in the scope, in which they provide the legal assistance or tax advisory services pertaining to the purchase or sale of real estates to the customer. These entities should fulfil all anti-money laundering and counter-terrorism financing obligations imposed by the act. The notaries drawing up the notary deed on transfer of ownership of the real estates, real estate agents as well as the advocates, legal councillors and lawyers

	from the abroad in the scope, in which they provide the legal assistance or tax advisory services pertaining to the purchase or sale of real estates to the customer are the OIs. The developers selling the real estates on the primary market are not the OIs. Although these OIs have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilling are still revealed. The level of awareness is diversified and depends primarily on the size of a given entity. Increasing the level of awareness of the notaries is the task of the Chambers of Notaries. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	Using various forms of transfer of ownership of the real estates for the purposes of effective money laundering is one of the most common methods of money laundering. This method is widely available, inexpensive and perceived by the perpetrators as highly attractive. Using various forms of transfer of ownership of the real estates for the purposes of money laundering requires neither specialist knowledge nor specific specialist skills. There are specialist professions, representatives of which – for a relatively low amount – assist in preparing the transaction of the transfer of ownership of a real estate and provide adequate services. This method of money laundering is frequently used by the organised crime. The organised crime groups frequently use the system of loans, credits, manipulate the valuation of assets, use the corporate vehicles and cash for the purposes of laundering the illicit proceeds. In many cases, the purchased real estates are reconstructed or renovated for the illicit proceeds and then re-sold at a much higher price. Creative accounting allows legalising the illicit proceeds. The GIFI receives information on using the method of transfer of ownership of real estates for money laundering purposes. CONCLUSION: Using various forms of transfer of ownership of the real estates for the purposes of money laundering poses a high threat of money laundering.

Table 62

Type of used services, financial products	Security on real estates and transferring of real estates as a contribution to the companies
General risk description	Using the forms of property securities on real estates and contributions in-kind to the companies for the purposes of money laundering
Risk occurrence scenario (i.e. possible risk occurrence example)	1. Purchase of fixed assets by the company was secured with the entry to the mortgage register of real estates. Since the company was a subsidiary company, the instalments were paid by the parent company having its seat in a tax haven. The fixed assets acquired by the company were purchased from clean funds in the form of a bank loan. 2. A foreign company with its seat in one of the tax havens gains credits secured on mortgage of the investment real estate. The mortgage of this real estate acts also as the security for credit and loans of other persons. The proceeds of crime are transferred abroad to the a/m foreign company and return to Poland as the transfers on the account of this company in a Polish bank or as investment contributions (for example for purchase of real estates). Credits granted by the bank are legal funds, while payment of these credits and loans can be made by among others by seizure by the bank of the real estate acting as the security. 3. Entering into the preliminary agreement obliging to transfer of ownership of a real estate. A high contractual penalty for withdrawal was a component of this agreement. Since the parties (members of the organised crime group) act

	in collusion and the agreement is not executed, the paid contractual penalty is a form of legalising the illicit proceeds. 4. A member of an organised crime group purchases a real estate at the market price and contributes it to the commercial law company overstating its value. With regard to overstating of the value of real estate, the value of the company itself is also increased. The shares obtained with regard to contribution of the real estate to the company are then sold to the "dummy" investor or investors.
Level of vulnerability	2
Justification for the level of vulnerability	Having a real estate enables incurring credits or loans, securing these agreement by the entry to the mortgage register established for this real estate. The funds obtained for example from the banks are legal, since they originate from a known source. The credit or loan instalments can be paid with the funds from not necessarily legal sources. Payments in cash are available in many cases. The mortgage consists in the opportunity to secure a given receivable on areal estate and encumber this real estate with the right, under which the creditor may satisfy such claims from the real estate, regardless of whose property it has become, in priority to the personal creditors of the owner of the real estate. The mortgage is established at the time of entry into the mortgage register – this entry is therefore constitutive. The mortgage is presented in section IV of the mortgage register. The GIFI has relevant access to the system of Electronic Mortgage Registers. The mortgage loans are available to an adult person, being the owner or co-owner of the real estate serving as a loan security. The mortgage can encumber the ownership right to the real estate (including lands), cooperative right to an apartment, perpetual usufruct right, right to a single-family house (in housing cooperative). The mortgage secures the mortgage loan up to a specific amount. The mortgage value is the maximum amount, in which the creditor may satisfy its claims from real estate encumbered with a mortgage. The loan may be granted by any entity with legal capacity, while the credits may be granted only by the banks and cooperative savings and credit unions (SKOK). The banks granting the mortgage secured credits are the OIs. Not all loan-granting entities are the OIs. Although the banks are aware of their AML/CFT obligations and apply customer due diligence, the controls continue to reveal the deficiencies in this area. With regard to pending military conflict in Ukraine, proper identification and verification of the Ukrainian refugees, interested in using the products available on the financial market, poses a particular challenge related to the proper application of customer due diligence measures. Due to pending military conflict, acquisition of a broader spectrum of documents confirming the customer's identity or reliability is impeded. There are also serious problems with identification and verification of persons having no documents at all or having documents such as internal passport in Cyrillic. Correct transcription of such documents into Latin alphabet is extremely hindered. In addition, the language and cultural barrier between the obligated institutions' staff and the refugees using the bank account makes identification of untypical customer behaviours difficult, which refers both to a customer willing to open for example a bank account and the customer making a transaction. The language and cultural barrier significantly affects proper identification of the increased risk factors. It acts as a behavioural factor, which makes it difficult to properly assess the responses provided by the customers – refugees in the problematic issues, which require additional information or documents. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information. It is highly probable that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3

Justification for the level of threat	Using the forms of property securities on real estates and contributions in-kind to the companies for the purposes of effective money laundering is one of the most common methods of money laundering. This method is widely available, inexpensive and perceived by the perpetrators as highly attractive. Using the forms of property securities on real estates and contributions in-kind to the companies for the purposes of money laundering requires neither specialist knowledge on the banking system and commercial low, nor specific specialist skills. There are specialist professions, representatives of which – for a relatively low amount – assist in preparing the credit application with the use of forms of property securities on real estates or application for contribution ink-kind to the company and provide the adequate services. This method of money laundering is frequently used by the organised crime. The organised crime groups use it frequently, and pay for the instalments with illicit cash to launder money. In many cases, as a adopted element of money laundering, the mortgage secured real estates are seized by the bank. The GIFI receives information on using the method of property securities on real estates and contributions in-kind to the companies for the purposes of money laundering. Conclusion: Using the forms of securities on real estates and contributions in-kind to the companies for the purposes money laundering poses a high threat of money laundering.

Terrorism financing

Table 63

Type of used services, financial products	Transfer of ownership of real estates and lease of real estates
General risk description	Using the sale of real estates and lease of owned real estates for the purposes of terrorism financing.
Risk occurrence scenario (i.e. possible risk occurrence example)	1. A real estate owned by a company run by the members of one of the ethnical groups is sold. A part of the sale amount, in effect of the accounting practices in the company, is transferred for terrorist activity. 2. The members of one of the ethnical groups in Poland purchased for the funds obtained from the abroad a real estate intended for lease. Most of income from lease is transferred to the terrorist organisations operating in the fatherland of the members of this group.
Level of vulnerability	2
Justification for the level of vulnerability	Transfer of ownership of real estates requires a notary deed. Without such deed, the concluded agreement shall have no legal effect. The basic evidence of existence of the ownership right of a real estate is the mortgage register. The GIFI has relevant access to the system of Electronic Mortgage Registers. Apart from the notary, the transfer of ownership of a real estate may involve the real-estate agents, as well as the advocates, legal councillors and lawyers from the abroad in the scope, in which they provide the legal assistance or tax advisory services pertaining to the purchase or sale of real estates to the customer. These entities should fulfil all anti-money laundering and counter-terrorism financing obligations imposed by the act. The notaries drawing up the notary deed on transfer of ownership of the real estates, real estate agents as well as the advocates, legal councillors and lawyers from the abroad in the scope, in which they provide the legal assistance or tax advisory services pertaining to the purchase or sale of real estates to the customer are the OIs. Although these OIs have certain awareness of their AML/CFT obligations, the deficiencies in their fulfilling are still revealed. The level of awareness is diversified and depends primarily on the size of a given entity. Increasing the level of awareness of the notaries is the task of the Chambers of Notaries. On the other hand, the lessor of a real estate

	does not need to be its owner. The lessor does not need to have a limited property right to the leased apartment. The lessor does not need to be the owner of the object of lease, since entering into the lease agreement is not treated as disposal of the ownership right. The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on the sale of real estates. In the case of lease, such knowledge is hardly available. There is low probability that the case of money laundering in the scope of the analysed scenarios will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted. However such option is available to the cooperating units, which monitor the extremist environments. The national and international cooperation of the public administration authorities is at a relatively good level. The existing legislation corresponds to the scope of the analysed risk to a large extent.
Level of threat	3
Justification for the level of threat	Using the sale of real estates and lease of owned real estates for the purposes of terrorism financing is one of the methods of terrorism financing. It is widely available, inexpensive and perceived by the perpetrators as rather attractive. Using the sale of real estates and lease of owned real estates for the purposes of terrorism financing requires neither specialist knowledge on the banking or financial system, nor specific specialist skills. There are specialist professions, representatives of which – for a relatively low amount – assist in preparing the transaction of transfer of ownership of the real estates and provide the adequate services. This method of terrorism financing is frequently used. Creative accounting enables hiding the transfer of a part of the amount from sales of real estates for the terrorism financing purposes. The GIFI receives little information on using this method of transfer of ownership of real estates or lease of real estates for the purposes of terrorism financing. CONCLUSION: Using the sale of real estates and lease of owned real estates for the purposes of terrorism financing poses a high threat.

The real estate sector is not only the one of the essential investment markets for the national and global business entities, but – due to its features – attracts also the organised crime groups, which use this sector for illegal activity or launder the proceeds of crime. Situation on the real estate market is of significance from the perspective of stability of the financial system and macro-economic stability of the state[101]. The economic and financial condition of developers and the construction companies, evolution of the offer and transaction prices on the primary and secondary real estate markets, situation on the commercial real estate market, office and commercial market, relationships between the prices of apartments and household incomes are also of importance. The criminal activity in the real estate sector may lead to its destabilisation and in effect to the destabilisation of the state economy. In certain countries, such destabilisation contributes to the increase in the real estate prices, making the apartments inaccessible to many people, which in turn affects the society and undermines the rule of law.

The "Raport o sytuacji na rynku real estates mieszkaniowych i komercyjnych w Polsce" (*Report on the situation on the residential and commercial real estate market in Poland)* published by the National Bank of Poland (NBP) on an annual basis, provided in its 2021 edition the statistical data on the Polish real estate sector. According to these data, the estimated value of the residential real estate market in Poland amounted to approx. PLN 5.6 trillion as of the end

[101] Raport o sytuacji na rynku nieruchomości mieszkaniowych i komercyjnych w Polsce w 2021 r., National Bank of Poland, 2022

of 2021, compared to PLN 4.9 trillion in 2020. The Estimated value of the commercial real estates reach approx. PLN 355 billion compared to PLN 314 billion in 2020. The value of residential real estates as of the end of 2021 corresponded to approx. 215% of GDP, while of commercial real estates to approx. 14% GDP (211% and 13% in 2020, respectively). According to the NBP estimations, the residential apartment resources in Poland amounted to approx. 15.3 million in 2021. The number of residential apartment resources per 1000 inhabitants increased (approx. 400 compared to 392 in 2020), so as the average usable space of the apartment per capita (approx. 30.0 sqm compared to 29.2 sqm in 2020). The average number per apartment decreased (2.50 in 2021 compared to 2.55 in 2020). In 2021, 97.5 thousand single-family one-dwelling houses were commissioned in Poland, i.e. by 18.5% more than one year earlier. The financing sources of the developers in 2021 (on average quarterly basis) included mostly the equity (approx. 43%), prepayments made by the customers (approx. 20%) and liabilities towards the contractors (approx. 24%), and additionally credits of approx. 6% and debt securities of approx. 7%.

The financial sector is of the key importance for the real estate sector, since it guarantees the liquidity of this market and valuation of the real estate values. In addition, the financial sector has a significant exposure to the real estate market. As of the end of 2021, the assets of the banking sector in the form of household credits for residential real estates amounted to approx. 38.8% of credits in total (i.e. increased by 0.8 pp. compared to 2020) and accounted for approx. 20.0% of banks' assets (i.e. decreased by 0.4 pp. compared to 2020). According to the Credit Information Bureau (BIK) data, in the 1st half of 2020 the Poles incurred credits and loans for the total amount of PLN 79.8 billion i.e. borrowed by PLN 8.7 billion less compared to the same period a year earlier. The greatest drops were recorded in the mortgage loans sector, i.e. by approx. 30% less[102].

Pursuant to the Polish regulations, transferring ownership of the real estate is made in the same moment, in which the purchaser signs the purchase agreement for this real estate. However, according to the legal requirements, the agreement of transfer of ownership of the real estate is formally valid only when it is concluded in a form of a notary deed. Entry into the mortgage register, upon signing of the agreement, is of declaratory nature.

The following entities are the obligated institutions professionally operating on the real estate market and identify the risks of money laundering and terrorism financing linked with business relationships or an occasional transaction and assess the level of the identified risk. These include the notaries – in the scope of the activities taken in the form of a notary deed, covering among others transferring ownership of assets, including sales, exchange or donation or movable property or real estate; entering into the agreement of distribution of the estate, abandonment of joint ownership of the property, life estate contract, pension for transfer of ownership of the real estate and distribution of property, […] contribution in-kind upon establishment of a company. These are also the advocates, legal councillors, foreign lawyers, tax advisors in the scope, in which they provide legal assistance or tax advisory services on the purchase or sale of real estate, undertaking or its organised part to the customer. Since 31 July 2021, the legislator has extended the catalogue of obligated institutions by introducing the provision that the real estate agent is an obligated institution in the meaning of the *Act of 21*

[102]https://direct.money.pl/artykuly/porady/kredyt-a-pozyczka-czym-sie-roznia,128,0,1658496, access on 03.09.2023

August 1997 on real estate economy, excluding the agency in trade in real estates aimed at conclusion of the lease or rental agreement of the real estates of their part, in which a monthly rent was determined in the amount lower than the equivalence of EUR 10,000.

Vulnerability of the sector

The transactions being the money laundering transactions on the real estate market are formally no different than fully legal transactions on this market. The criminal nature of money laundering transactions is manifested when the objective of these transactions and illegal sources of origin of funds used in these transactions are revealed.

Due to its features, which include the market size (the value of the residential real estate sector in Poland amounted to approx. 5.6 billion as of the end of 2021), international nature of transactions, geographical division and numerous factors affecting the local price of real estates – the real estate sector is considered relatively vulnerable to money laundering. This vulnerability of the real estate sector results among others from high nominal value of transactions on this market. High value of real estates in commercial trade makes the real estates attractive for criminals or criminal organisations attempting to hide large amounts of illicit proceeds. The valuations of real estate on this market may be manipulated. Introduction of some falsified data to a recognised real estate valuation algorithm allows for discretionary estimation of the value of real estates. In this way, one can understate the estimated value of the purchased real estate and purchase it below the actual market value. In the case of money laundering, this does not mean however that the seller of a real estate is unaware or deceived as to the actual value of real estate. The real estate purchase transaction is simply settled in two stages. In the first stage, the official understated value of real estate is paid, while in the second – the price of transfer of ownership of the real estate is supplemented by, for example, cash outside the legal trade, up to the market value. In this way, the money launderer on the real estate market becomes the owner of a real estate of a much higher value than the officially paid price. Further dispositions on the real estates, such as e.g. sale or exchange, take place at the market values. In this manner, the funds used to purchase a real estate are legalised (outside the official trading).

Valuation of the real estates in Poland is performed in the form of a property valuation report. The property valuation report is the opinion on the value of a real estate made by the certified property valuator. The property valuation report is considered the official document and is officially recognised in various administrative cases. Its form and content is laid down by the "Regulation of the Council of Ministers on valuation of intangible property and preparation of the property valuation report". This document is valid for the period of 12 months from the date of preparation thereof. The property valuation report contains information of significance for valuation by the property valuator – description of property with a view to the physical, legal and functional aspects. The report is accompanied by important documents used for its preparation. It is made in writing and must be signed by the author. The property valuation report can be drawn up only by the certified property valuator.

The increased vulnerability of the real estate sector related to money laundering and terrorism financing is also affected by the opportunity to use cash in payments. Vulnerability to money laundering is increased each case of cash payments when transferring the ownership right of the real estates, since tracking of the source of funds used for the transaction becomes more difficult. It should be noted however that in any case of payments by an operator for any goods

(in this case for the real estate) in cash or of accepting such payment in the amount exceeding the equivalence of EUR 10,000 it becomes the obligated institution in the meaning of the *Act on counteracting money laundering and financing of terrorism*. Such operator is then obliged to designate a person responsible for implementation of the statutory obligations, performing the risk analysis, implementing the relevant procedures and apply customer due diligence measures consisting among others in the identification of customer, beneficial owner, politically exposed persons as well as assessment of business relationships of the customer. In addition, the obligated institutions are obliged to submit information on transactions to the GIFI. Cash is also used, when real estates purchased for money laundering purposes are reconstructed or renovated for the proceeds of crime and the resold at a much higher price.

Some transactions aimed at transfer of ownership of a real estate may be of more complicated nature, resulting for example from the fact that the real estate is purchased by a greater number of persons or entities. The implemented anonymisation elements, impeding monitoring of business, family or professional relationships of the entities making the transactions, increase the vulnerability of the transactions of transfer of ownership of real estates to money laundering or terrorism financing. Monitoring of transactions and checking the existence of the potential capital, organisational or personal links between the parties may be impeded, in particular in the case of participation of the entities subsidiary to the entities from the other jurisdictions in the transaction.

Monitoring of business relationship of the customers, including analysis of transactions performed within the business relationships in order to ensure that these transactions are compliant with the knowledge of the obligated institution on the customer, type and scope of its activity, and compliant with the risk of money laundering and terrorism financing linked with this customer, is - in the case of the obligated institutions handling the transactions of transfer of ownership of the real estates involving the contractors – significantly impeded.

Vulnerability of the real estate market to money laundering or terrorism financing is affected by the provisions of the *Act on counteracting money laundering and financing of terrorism*. They impose numerous obligations on the obligated institutions handling the transactions of transfer of ownership of real estates, concerning the application of customer due diligence in trade in real estates. Customer due diligence undertaken by these obligated institution should be adequate to the size of entity and scope of its activity. The customer due diligence measures in the area of AML applied by the staff of the obligated institutions include among others identification of customer; verification of the customer identity; identification of the beneficial owner in the Central Register of Beneficial Owners (CRBO); monitoring of discrepancies between the CRBO and findings of the obligated institution, determination of the ownership and control structure in the case of a customer being a legal person or organisational unit without legal personality; assessment of business relationships of the customer; continuous monitoring of transactions and business relationships linking the obligated institution with its customers.

Vulnerability of the real estate sector for the purposes of money laundering and terrorism financing is also affected by the appropriate application of the risk-based approach under the KYC. Since some jurisdictions enable a certain level of anonymity in the real estate purchase transactions, revealing no identity of the owner or benefiting from the intermediation of special purpose companies, and since the other jurisdictions require no detailed information on the

source of funds for the purposes of real estate purchase, Poland needs to put emphasis on the elements of tax and legal engineering introduced by the contractors to the transactions to hide the origin of the funds. Identification of the beneficial owner of the transaction of transfer of ownership right of the real estate is in some cases relatively easy, while in the other cases highly complicated. Using in the transactions of so called investment vehicles in a form of frequently multi-level offshore companies, trusts or shell companies enables money laundering by means of the investments in real estates, which become in such cases a carrier of illicit proceeds.

Banks, which grant credits for the purchase of real estates, play an important role on the real estate market. From the perspective of real estate sector vulnerability to money laundering but also from the point of view of security of the bank's operation, one of the crucial issues is sustainable policy of financing the transactions on the real estate market, including in particular the valuation of security on real estates. In order to mitigate the effects of the potential crisis situations, ensure effective management by the banks with regard to the risk related to acceptance of mortgage-based securities on real estates and the need for reliable and complete information on the real estate market, up-to-date or historical data, which would demonstrate the changes on this market in the long- and short-time perspective, the PFSA issued the new Recommendation J in March 2023. The Recommendation J refers to good practices in the area of collecting and processing by the banks of data on the real estate market contained in the internal (own) and external (inter-bank) databases, supporting the process of risk management related to the exposures of mortgage-secured credits. A bank, adapting its operation to the Recommendation J, follows the provisions of law, in particular of the *Act of 29 August 1997 on covered bonds and mortgage banks* and of the *Act of 21 August 1997 on real estate economy.* The Recommendation J applies to all mortgage-secured credits granted from the date of its entrance into force.

The public administration authorities have knowledge on the ML/FT risk in this scope. The GIFI is capable to collect and analyse information on this type of services. It is highly probable that the case of money laundering or terrorism financing will be detected and then in effect of investigation/inquiry the perpetrators will be prosecuted and convicted.

The national and international cooperation of the public administration authorities is at a relatively good level.

The existing legislation corresponds to the scope of the analysed risk to a large extent.

Threats in the sector

Money laundering in the real estate sector encompasses the threats both at the national and global level. Since this form of money laundering requires no specific specialist knowledge, there are professions handling the transactions on the real estate market, the transaction costs borne by the contractors are relatively low, according to the forensic theory of reasonable choice, the investment on the real estate market in order to legitimise the illegal proceeds is highly attractive. From these reasons, this method of money laundering continues to attract the interest of the international organised crime group.

Money laundering on the real estate market may also have a negative impact on the real estate market in a given state, resulting in its instability due to uncontrolled changes of the prices of real estates or construction materials, development or stagnation of the construction materials industry, change in the business activity of the construction sector companies, and as such may

affect the development of this country. The investments in real estates lead to the inflow of funds to a given country, which significantly affects the investment decisions made by the potential purchasers and sellers of the real estates. This affects also the investment decisions of the state and self-governmental authorities. Such economic decisions made in effect of a significant exposure of illegal proceeds to the real estate market, bearing an investment bias, pose a threat to the interests of any state.

Establishing of complex capital structures aimed at impeding or preventing reaching the actual owners (beneficial owners) for the purposes of transactions on the real estate market poses a threat. Internationalisation of such capital structures and their partial or complete location in the jurisdictions of poor transparency impedes their identification by the KYC procedures. In some cases, only the activities of the specialist supervisory authorities or law enforcement authorities enable revealing the actual holders of funds and detecting the traces of money laundering on the real estate market. Such non-transparent capital structures introduce the element of anonymity to the transactions on the real estate market.

The element of anonymity as the component of threat in the transactions on the real estate market introduces also the opportunity of using cash in the transactions on this market. The organised crime groups operating on the real estate market use cash from illegal activity for the purposes of money laundering – and not only as the form of payment for a real estate. In many cases, the real estates purchased for the purposes of money laundering are in poor technical condition. After the purchase, they are reconstructed or renovated for the proceeds of crime and then resold at a much higher price. The construction companies participating in the construction works, construction material stores, construction workers – are the entities willingly accepting the payments in cash. In many cases, a part of activity of these entities is conducted in a gray market. Creative accounting allows legalisation of the illicit proceeds. The threat in the real estate sector is also increased by the fact that the value of real estates subject to money laundering, in particular in attractive locations, is extremely high. The investments of the proceeds of crime in real estates can be treated as relatively easily accessible form of allocating or storing large amounts of money in the form of a safe, yet sometimes difficult to trade asset.

The assessment of threat of money laundering and terrorism financing to the real estate is also affected by lack of appropriate supervision and control over this market. A standard control of performance by the obligated institutions of their obligations in the area of anti-money laundering and counter-terrorism financing is generally insufficient in terms of the real estate market. Only with regard to the notaries such control is performed by the presidents of the courts of appeal. In the case of the other professions, the control is performed by the heads of the customs and tax control offices and by the GIFI

Using the sale of real estates and lease of owned real estates may also be one of the methods of terrorism financing. In such case, the funds may origin primarily from a legal agreement for a sale of real estate or legal lease agreement, concluded by the persons or other entities supporting the extremist or terrorist groups. According to the GIFI information, the Internal Security Agency, in the course of its operational and analytical activities, recorded the cases of investing the funds acquired by the members and supporters of terrorist groups at the territory of Poland, including in the associated business entities (or with the aim to establish another ones), income from which is then allocated to a given organisation or for the purchase of real estates by these

persons (including without any economic justification – for example in poor technical condition).

Averaged level of threat of the real estate sector – ML – 3.0 and FT – 3.0

Averaged level of vulnerability of the real estate sector – ML – 2.0 and FT – 2.0

Estimated level of probability for the sector – ML – 2.40 and FT – 2.40

The level of risk is ultimately determined by the combination of threat versus vulnerability. The risk matrix determining this level of risk is based on the weighting of 40% (threat) + 60% (vulnerability) – provided that the vulnerability component is more capable of determining the level of risk. It is assumed that the level of vulnerability may increase the attractiveness, and therefore the intent of the perpetrators to use a modus operandi concerned - which ultimately affects the level of threat. The level of risk of the sector, with consideration to the estimated vulnerability and consequences (coefficient of 2.5 for ML and 1.5 for FT), is determined in accordance with the national risk assessment methodology – annex no. 1.

FT risk of the real estate sector – 2.04	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high
ML risk of the real estate sector – 2.44	
1 – 1.5	Low
1.6 – 2.5	Medium
2.6 – 3.5	High
3.6 – 4	Very high

CONCLUSION 1: The level of risk of using the real estate sector for the purposes of terrorism financing in Poland is at a medium level.

CONCLUSION 2: The level of risk of using the real estate sector for the purposes of money laundering in Poland is at a medium level.

Mitigation of the identified risks:

In order to mitigate the probability of using the real estate goods for the purposes of money laundering or terrorism financing, it is reasonable to take appropriate actions or applying the measures aimed at mitigating the risk of money laundering and terrorism financing. This applies

in particular to the entities handling the transactions on the real estate market being the OIs. Applying the relevant mitigation measures in the anti-money laundering process is one of the basic aspects of ensuring the effective protection of these institutions against the legal, financial and reputational risks.

In the real estate market, the level of awareness of money laundering and terrorism financing risk is highly diversified and depends in particular on the size of a given market entity and its structure. These factors determine the access of the staff of the OIs providing services for the real estate market to the state-of-the-art information and training tools. The above requires a greater focus of these OIs on the verification of the source of origin of the customer's assets used in the transaction of transfer of ownership of a real estate and proper identification of the beneficial owner. Taking by the OIs of the necessary actions to verify the customer's identity and to determine the ownership and control structure in the case of a customer being a legal person or an organisational unit without legal personality is necessary practically in each case of transaction of transfer of ownership of a real estate on the market.

The obligated institutions operating on the real estate market should put particular attention in the cases, where the monitoring of the business relationships of the customer reveals its business links/relations with the jurisdictions of higher risk of money laundering and terrorism financing, and in particular when the transactions use so called investment vehicles covering the offshore companies, trusts, etc.

The obligated institutions should put particular emphasis on obtaining information from the customer on the purpose and intended nature of the business relationships and should monitor the business relationships on an on-going basis and – in justified situations – request the customer to submit information and documents on the source of origin of assets. Especially in the case of providing by the obligated institutions from the notary sector of the services covering the sale of enterprises (covering also the real estates) or contributions to the capital companies (in the form of real estates), performing the assessment of economic justification of these activities is reasonable. The obligated institutions should put particular attention to the acquisition of relevant up-to-date information on the customer and in the course of business relationships also on the transactions made for and by the customer.

When the level of awareness of the money laundering and terrorism financing risk in the real estate sector is highly diversified, the OIs operating on this market should make all efforts enhancing the level of this awareness, in particular by increasing the level of the staff skills in the area of analysing the warning signals triggered by suspicious transactions. Training the staff in the area of anti-money laundering and counter-terrorism financing enables understanding and identification of the potential threats in the sector, of which they are an important element.

It is recommended to develop the advanced IT tools and systems supporting the implementation of the objectives of anti-money laundering and counter-terrorism financing and deploy such solutions by the entities, which have not used them yet.

The real estate market should establish and document clear and transparent anti-money laundering and counter-terrorism financing procedures, specifying the warning thresholds, which indicate the need for further analysing of the transactions and applying the customer due diligence measures. A particular focus should be on the geographic and geopolitical factors, which may indicate a higher risk of money laundering or terrorism financing, such as unstable

political situation or a military conflict, which can be best illustrated by the Russian warfare against Ukraine in recent years.

Due to highly diversified level of awareness of the money laundering and terrorism financing risk in the real estate sector, regular performance of audits and internal tests, assessing the effectiveness of the KYC programmes applied by the OIs and enabling identification of the area requiring improvements is of importance.